National Security Systems Public Key Infrastructure

Department of Defense
Registration Practice Statement

Version 5

13 June 2012

In Compliance With

CNSS Instruction No. 1300
National Security Systems Public Key Infrastructure
X.509 Certificate Policy

Version 1.1

June 2011

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 INTRODUCTION

See *CNSS Instruction No. 1300, Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy* [CNSSI 1300].

1.1 OVERVIEW

See [CNSSI 1300].

1.1.1 Certificate Policy

This Registration Practice Statement (RPS) conforms to [CNSSI 1300].

1.1.2 Relationship between the Certificate Policy and the Certification Practice Statement

This RPS conforms to [CNSSI 1300].

1.1.3 Scope

This RPS applies to Registration Authority (RA) Officers from the CC/S/A that participate in the issuance process for all certificates issued to named individuals that assert a [CNSS 1300] Policy Object Identifier (OID) (see Section 1.2). This RPS also applies to the individuals responsible for these certificates, persons operating an RA System, and Trusted Agents (TAs) appointed by an RA Officer operating under this RPS.

It does not address requirements that are addressed by the CA specific information. That is addressed in the *National Security Systems (NSS) Public Key Infrastructure (PKI): Department of Defense (DoD) Subordinate Certification Authority System (CAS) Certification Practice Statement (CPS)* [CAS CPS]. It also does not address process for issuance of certificates as described in the *NSS PKI DoD Non Person Entity (NPE) CAS CPS* [NPE CAS CPS]. It does include nomination, credentialing and security controls for the NPE Verifying Officials (NVOs).

1.1.4 Interoperation with CAs Issuing Under Different Policies

See [CNSSI 1300].

1.2 DOCUMENT NAME AND IDENTIFICATION

The official title of the RPS is the "*Department of Defense Registration Practice Statement.*"

This RPS is involved in the issuance of certificates that assert the following Policy OIDs, defined in [CNSSI 1300]:

id-cnss-policies:: = {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) cert-policy(1) cnss(21)}

id-CNSS-software	ID::={id-CNSS-policies (1)}
id-CNSS-hardware	ID::={id-CNSS-policies (2)}
id-CNSS-device	ID::={id-CNSS-policies (3)}

1.3 PKI PARTICIPANTS

1.3.1 CNSS Policy Management

See [CNSSI 1300].

1.3.1.1 NSS PKI Policy Management Authority

See [CNSSI 1300].

1.3.1.2 NSS PKI Member Governing Body

See [CNSSI 1300].

1.3.1.3 Agency NSS PKI Management Authority

The Department of Defense (DoD) Agency NSS PKI Management Authority (ANMA) is the Director, DoD Public Key Infrastructure (PKI) Program Management Office (PMO). ANMA responsibilities are specified in [CNSSI 1300]. DoD signing CAs subordinate to the NSS PKI Root CA conform to the practices specified in [CAS CPS].

DoD implements RPSs. The ANMA performs a compliance analysis of RPSs and determines whether they meet the requirements of [CNSSI 1300] and [CAS CPS].

1.3.1.4 Agency NSS PKI Point of Contact

Not applicable.

1.3.2 Certification Authority System

Not applicable.

1.3.3 Registration Authority

An RA is an entity authorized by the CAS to collect, verify, and submit information provided by potential Subscribers which is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function. Unless expressly stated otherwise, RA requirements are imposed on all RA components of the NSS PKI. RA operations are performed in accordance with [CAS CPS] and this RPS. The RA is responsible for the following:

- Control over the registration process;
- The identification and authentication process;
- The revocation, suspension and restoration process; and,
- The Key Recovery process.

1.3.3.1 RA System

The RA System includes hardware and software that is used by the RA Officer in support of the CAS in collecting and formatting information that is to be used in certificate issuance, certificate revocation, and key recovery. External databases that are used to support the verification of Subscriber or Requestor information are not considered part of the RA System.

1.3.3.2 RA Operations Staff

RA components are operated and managed by individuals holding trusted roles. Specific responsibilities for these roles, as well as requirements for the separation of duties, are described in Section 5.2. RA Operations Staff are designated as holding a trusted role.

1.3.3.3 RA Officer

An individual who is responsible for any of the duties of certificate issuance, certificate revocation, or key recovery is designated as an RA Officer. Duties may be performed by the same individual, or may be separated across different roles. RA Officers are designated as holding a trusted role.

Not all RA Officers have the same authority within the PKI. Some RA Officers may be specifically designated only to perform duties as an NVO. NVOs approve issuance of System and Device certificates via the NPE Registry. Some, designated as Local Registration Authorities (LRAs), only have authority to perform the Name certificate registration function of an RA. Individuals designated as LRAs do not have the authority to approve Code Signing, System or Device certificates not issued via the NPE Registry; revoke, suspend, or restore certificates; or perform key recovery operations. Any LRA may also be designated to perform NVO functions. Except as noted above, all references to RA Officers include LRAs and NVOs. Some RA Officers have privileges on the CA to do registration/revocation functions. Other RA Officers have privileges to do Key Recovery functions. An RA Officer may have privileges to perform both functions. All RA Officers that have revocation privileges also are designated to perform NVO functions. The RA Officer Nomination memorandum states which functions the RA Officer will perform.

1.3.4 Trusted Agent

A TA is an individual explicitly aligned with one or more RA Officers who has been delegated the authority to perform a portion of the RA function (e.g., a TA may perform identity proofing of certificate applicants for a requestor who cannot appear in person before an RA Officer). A TA does not have privileged access to CAS components to authorize certificate issuance, certificate revocation, suspension, restoration, or key recovery. Instead, the TA provides information to the RA Officer in a secure fashion. No request submitted by a TA is implemented until approved by an RA Officer. TAs are designated as holding a trusted role and all have an *id-CNSS-hardware* Name certificate that they use for all interaction with the RA Officer.

1.3.5 Subscriber

A Subscriber is the entity whose name appears as the subject in a certificate. The NSS PKI supports issuing certificates to three types of Subscriber: Name, Role, and System or Device. Unless otherwise specified, statements for Subscriber apply to all three types. Each Certificate has a person who is responsible for the private key associated with a certificate, known as the PKI Sponsor, who asserts that the certificate and associated private key are being used in accordance with [CNSSI 1300]. All PKI Sponsors have an *id-CNSS-hardware* Name Signature certificate. Each of the types of Subscriber has an associated PKI Sponsor. Table 1-1 shows the PKI Sponsor for each type of Subscriber.

Table 1-1: Subscriber Types

Subscriber Type	PKI Sponsor
Name	Individual named in the certificate
Role	Individual authorized to use certificate or designated individual responsible for management of Role certificates
System or Device	Designated individual responsible for system or device keys

CASs are sometimes technically considered Subscribers in an NSS PKI. However, the term Subscriber as used in this document refers only to those entities that request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.5.1 Name Subscriber

Name certificates contain an individual name as the subject. Name certificates are tightly coupled with the individual named in the certificate. Name certificates are issued to Federal Government employees, contractors, and affiliates. The PKI Sponsor for a Name certificate is the individual named in the certificate.

1.3.5.2 Role Subscriber

Role certificates contain a role, group, or organization name as the subject; they do not contain the name of an individual in the *Distinguished Name* (DN) field. The PKI Sponsor for a Role certificate is an individual who is explicitly responsible for managing access to the private key associated with the certificate. In addition, the PKI Sponsor is responsible for establishing technical or procedural controls and managing access to the private key associated with the certificate. Code signing certificates are special Role certificates that are used to sign code.

1.3.5.3 System or Device Subscriber

System or Device certificates contain a system or device name as the subject. Systems and devices may be virtual or actual physical entities. Systems and Devices are also referred to as NPEs. Examples of Systems or Devices are workstations, guards, firewalls, routers, web server, database server, and other infrastructure components. The PKI Sponsor for a System or Device certificate is an individual who shall be explicitly responsible for managing access to the private key associated with the certificate. System and Device certificates may be issued as specified in the RPS or as specified in the DoD NPE CA CPS [NPE CA CPS].

1.3.6 Relying Party

A Relying Party uses a Subscriber’s certificate to verify or establish one or more of the following:

- The identity and status of an individual, role, or system or device
- The integrity of a digitally signed message
- The identity of the creator of a message
- Confidential communications with the Subscriber

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. A Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate (such as Certificate Policy OID identifiers) to determine the suitability of the certificate for a particular use.

Relying Parties may base the reliance they choose to place on a certificate on the factors such as the amount and type of inherent risk of an activity, the consequence of failure, and the use of risk mitigation controls.

1.3.7 Other Participants

An RA Officer operating under this RPS requires the services of at least one Systems Administrator (SA), Information Assurance Officer (IAO) and Compliance Auditor. RA Officers, SAs, IAOs, TAs and Compliance Auditors are the entities described in this document designated as holding a trusted role. As such, they are required to meet the personnel controls identified in Section 5.3.

An RA Officer operating under this RPS who issues Role certificates relies on a Role Based Attribute Authority (RBAA). An RA Officer operating under this RPS who issues Code Signing certificates also relies on a Code Signing Attribute Authority (CSAA).

1.3.7.1 Systems Administrator (SA)

An SA is a person authorized to perform operations on the RA system that require privileged access.

1.3.7.2 Information Assurance Officer (IAO)

An IAO is the person responsible for providing security services that support the RA operation.

1.3.7.3 Compliance Auditor

A compliance auditor performs compliance audits as specified in Section 8.

1.3.7.4 Code Signing Attribute Authority (CSAA)

The CSAA is the entity within the CC/S/A authorized to appoint individuals to receive and use DoD issued code signing certificates. Within the CC/S/A, the commander/director of the organization that is responsible for execution of the RPS designates, using a means that can be authenticated, the CSAA to the CC/S/A RA Officer.

1.3.7.5 Role Based Attribute Authority (RBAA)

The RBAA is the entity within the CC/S/A authorized to appoint individuals to receive and use DoD issued Role certificates other than code signing certificates. Within the CC/S/A, the commander/director of the organization that is responsible for the role designates, using a means that can be authenticated, the RBAA to the CC/S/A RA Officer.

1.4 CERTIFICATE USAGE

See [CAS CPS].

1.4.1 Appropriate Certificate Uses

RA Officers and TAs ensure that PKI sponsors know that certificates issued by the NSS PKI are to be used to protect classified information SECRET or below within U.S. SECRET networks or information systems.

1.4.2 Prohibited Certificate Uses

RA Officers and TAs ensure that PKI sponsors know that certificates issued by the NSS PKI are not to be used to support transactions unrelated to United States (U.S.) Government business.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The DoD PKI PMO is responsible for administering this RPS. The CC/S/A organization that is responsible for the execution of this RPS is identified separately.

1.5.2 Contact Person

The DoD PKI PMO is responsible for maintaining this RPS. The CC/S/A contact information and address for the organization that will use this RPS is identified separately.

1.5.3 Person Determining CPS Suitability for the Policy

The DoD ANMA determines the compliance of this RPS with requirements of [CNSSI 1300] and [CAS CPS].

1.5.4 CPS Approval Procedures

This RPS is submitted to the DoD Certificate Policy Management Working Group (CPMWG) for compliance analysis against the requirements of [CNSSI 1300] and [CAS CPS]. If deemed compliant, the CPMWG forwards the RPS to the DoD ANMA for approval.

1.5.5 Waivers

Waivers are not granted under any level of assurance. Variation in CAS and RA practices are either deemed acceptable under a current Certificate Policy OID, or the ANMA submits a change request to [CNSSI 1300]. If neither is possible, DoD may establish a new Certificate Policy OID for the non-compliant practice under the NSS PKI.

1.6 DEFINITIONS AND ACRONYMS

See Appendices B and C.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Not applicable.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

Not applicable.

2.3 TIME OR FREQUENCY OF PUBLICATION

Not applicable.

2.4 ACCESS CONTROLS ON REPOSITORIES

Not applicable.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

For Name and Role certificates, the RA Officer provides elements of the DN and other fields to the CA for inclusion in the certificate based on the certificate type. For System or Device certificates, the RA Officer verifies or edits the DN and other fields in the certificate request posted to the CA by the PKI Sponsor.

3.1.2 Need for Names to be Meaningful

RA Officers ensure that the subject name identifies the entity to which the certificate is assigned in a meaningful way. The RA Officer validates that an affiliation exists between the Subscriber and any organization identified by any component of any name in its certificate. The RA Officer uses local knowledge (direct or via a TA) to verify organizational affiliation.

The common name (CN) represents the Subscriber. The remainder of the DN represents the subscriber's organization affiliation. For Name certificates, the RA Officer ensures that the common name is understandable for humans. For Name certificates, this will typically be a legal name. For Role certificates, this will typically be the formally recognized name of the role, group, or organization. For System or Device certificates, this typically will be a fully qualified domain name or an application name.

For Name certificates, the RA Officer interface to the CA restricts the name choices available to the RA Officer to those within DoD's approved name space.

For Role, System and Device certificates, the RA Officer verifies that the requested DN is within DoD's approved name space prior to approving the certificate for issuance.

Note that the LRA Server only allows spaces or hyphens to be used as separators in CN fields.

3.1.2.1 RA Officer Certificate Name

RA Officers who have revocation or recovery privileges will have certificates that contain names with the following form:

cn=RA.<last_name>.<first_name>[.<middleName|middleInitial>][.<generation_qualifier>].< EDIPI>, ou=<CC/S/A>, ou=DoD, ou=NSS, o=U.S. Government, c=US.

An RA Officer that will function only as an NPE Verifying Official (NVO) will have certificates with the following form:

cn=NVO.<last_name>.<first_name>[.<middleName|middleInitial>][.<generation_qualifier>].< EDIPI>, ou=<CC/S/A>, ou=DoD, ou=NSS, o=U.S. Government, c=US.

The EDIPI is a ten-digit number assigned to individuals by the Defense Enrollment Eligibility Reporting System (DEERS).

3.1.2.2 LRA Certificate Name

RA Officers approve the issuance of certificates to LRAs with the following form:

cn=LRA.<last_name>.<first_name>[.<middleName|middleInitial>][.<generation_qualifier>].< EDIPI>, ou=<CC/S/A>, ou=DoD, ou=NSS, o=U.S. Government, c=US

3.1.2.3 Individual's Names

Most individual Name Subscribers will have certificates that contain names with the following form:

cn=<last_name>.<first_name>[.<middleName|middleInitial>][.<generation_qualifier>].< a ten-digit unique identifier number >, ou=<CC/S/A>, ou=DoD, ou=NSS, o=U.S. Government, c=US

Individuals performing as network system administrator Name Subscribers may have a specific Name certificate that has "ADM" pre-pended to the CN. These are referred to as "SA Name certificates."

The ten-digit unique identifier will either be the EDIPI which has been obtained from the Subscriber's S-ADR record or a Unique Identifier (UID) assigned by the registration system (e.g., LRA Server) during the registration process.

3.1.2.4 Device Certificate Names

The DN convention used for Devices issued via the manual process is:

cn=<XXXX>, ou=<CC/S/A>, ou=DoD, ou=NSS, o=U.S. Government, c=US

The cn= will be a Fully Qualified Domain Name. For Web Servers, the cn= must be the exact URI name by which the server is accessed by clients. Some NPEs are not sensitive to the cn= in the certificate and it serves only as a label.

For Devices that are accessed using multiple names, the primary Fully Qualified Domain Name will be used in the DN. If there is a Subject Alternative Name field, it contains the primary name and may contain alternate names.

3.1.2.5 System/Application Names

The DN convention used for System/Application certificates is:

cn=<application name>, ou=<CC/S/A>**,** ou=DoD, ou=NSS, o=U.S. Government, c=US

LRAs will assist RA Officer with privileges to issue manual system or device certificates in facilitating the issuance of certificates to applications using the System/Application certificate process. For applications, the PKI Sponsor provides the application name for the CN. This will be the name of the application as registered in the SIPRNET Defense Information Technology Portfolio Repository (DITPR).

3.1.2.6 Role-Based Certificate Names

Role-Based certificates fall into one of the three types discussed below. The cn= portion of the Distinguished Name (DN) is limited to 64 characters.

3.1.2.6.1 Role Certificates

A Role certificate is one which is issued to an individual filling a specific organizational role or function. The certificate will be issued in the name of the organization and role. The DN for Role certificates will contain a CC/S/A organizational unit (ou) component (e.g., ou=USMC). The complete DN for a Role certificate is:

> cn=<Organization_Name.Organizational_Component.Role_Name.UID>, ou=<CC/S/A>, ou=NSS, ou=DoD, ou=NSS, o=U.S. Government, c=US

The RA Officer will register Role Certificates. The common name (cn=) of the Role certificate will be entered into the certificate request in the fields provided by the TPS or LRA Server Interface (Organizational Name, Organizational Component, Role Name.)

The RBAA provides the Organizational Name, Organizational Component, and Role Name. The UID Block Identifier will be assigned in accordance with Section **Error! Reference source not found.**.

3.1.2.6.2 Group Certificates

A Group certificate is one which is issued to group of individuals for simultaneous use while filling a specific organizational function. The certificate will be issued in the name of the organization and group. The DN for Group certificates will contain a CC/S/A organizational unit (ou) component (e.g., ou=USMC). The complete DN for a Group certificate is:

> cn=<Organization_Name.Organizational_Component. Group_Name.UID>, ou=<CC/S/A>, ou=DoD, ou=NSS, o=U.S. Government, c=US

The RA Officer will register Group Certificates. The common name (cn) of the Group certificate will be entered into the certificate request in the fields provided by the LRA Server Interface: Organizational Name, Organizational Component, and Group Name.

The RBAA provides the Organizational Name, Organizational Component, and Role Name. The UID Block Identifier will be assigned in accordance with Section **Error! Reference source not found.**.

3.1.2.6.3 Code Signing Certificate Name

The DN convention for Code Signing Certificates is:

> cn=CS.<ORG Name>.<CSID>, ou=<CC/S/A>, ou=DoD, ou=NSS, o=U.S. Government, c=US

The CSAA provides the ORG Name. The Code Signer Identifier (CSID) is assigned to a Code Signing request by the CC/S/A's CSAA and may be composed of alphanumeric characters.

3.1.3 Anonymity or Pseudonymity of Subscribers

The RA Officer provides meaningful name information to the CA as specified in Section 3.1.2 for each type of certificate. See [CAS CPS] for CA responsibilities.

3.1.4 Rules for Interpreting Various Name Forms

The DoD implementation of the NSS PKI will only use the following name forms: DN, URI [Request For Comment (RFC) 3986], DNS [RFC 1034], Electronic Mail Address [RFC 5322[1]], Microsoft User Principle Name (UPN), X.500 Directory Name, or Globally Unique Identifier (GUID) (Microsoft implementation of [RFC 4122].) These name forms are interpreted in accordance with the applicable ISO and Internet standards.

3.1.5 Uniqueness of Names

Within DoD, the RA Officer ensures that Name and Role Subscriber names are unique, Name certificates use the EDIPI or UID within the CN.

For System or Device certificates, the use of the FQDN ensures it is unique to the system or device.

For application certificates, DITPR requires that the application name be unique within the CC/S/A. Combining this CN with the CC/S/A field, guarantees that the DN is unique.

For Role Certificates, the RBAA or CSAA ensures that the DN is unique within the CC/S/A prior to providing it to the RA Officer.

The LRA Server infrastructure automatically generates 10-digit UIDs beginning with the number 9 for Subscribers that do not have an EDIPI. The LRA Server implementation guarantees that no two Subscribers have the same UID.

If the RA Officer identifies any naming collisions, the RA Officer will investigate. If it is an EDIPI collision, the RA Officer forwards the issue to the DoD PKI Program Management Office (PMO) to engage with DEERS. Otherwise, the RA Officer works with the appropriate authority (e.g., RBAA) to resolve. Once the collision is resolved, the RA Officer revokes and re-issues the certificates of the persons or Roles impacted by changed CN.

3.1.6 Recognition, Authentication and Role of Trademarks

The RA Officer will not knowingly assign names that contain trademarks. The RA Officer need not seek evidence of trademark registrations nor in any other way enforce trademark rights.

[1] Many applications still incorrectly refer to this as an RFC 822 name. RFC 822 has been replaced.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

Proof of possession of private keys is a Subscriber responsibility to the CA as is described in [CAS CPS]; RA Officers have no responsibilities in this area except when acting as or for the Subscriber.

For Name and Role certificates issued under this RPS via TPS, either the PKI Sponsor is in possession of the token when the key is generated or the RA Officer executes key generation for the Subscriber and forwards the keyed token (i.e., token containing keys and certificates) to the PKI Sponsor as described in Section 6.1.2.

For Name or Role Certificates issued in software, either the PKI Sponsor is present when the key is generated or the RA Officer generates the key and forwards the P12 file to the PKI Sponsor as described in Section 6.1.2.

For System and Device certificates, the PKI Sponsor is present at the generation of the keys and posts PKCS 10 file to the CA through the CA interface. The PKCS 10 file containing the public key is signed by the corresponding private key.

3.2.2 Authentication of Organization Identity

The RA Officer validates that an affiliation exists between the Subscriber and any organization identified by any component of any name in its certificate.

RA Officer will support the issuance of Role certificates. The RA Officer will authenticate the PKI Sponsor, using the procedures in Section **Error! Reference source not found.** and this section. In addition, the RA Officer will verify that the PKI Sponsor applying for a role-based certificate is authorized to act in this role. The RBAA or CSAA provides the RA Officer with the necessary information for creation of the Role certificate.

3.2.3 Authentication of Individual Identity

For certificates issued via an RA Officer, the RA Officer verifies the PKI Sponsor applicant's identity information as specified below.

3.2.3.1 Authentication for Name Subscribers

The RA Officer authenticates the identity and the specified attributes for Name Subscribers through all of the following mechanisms prior to initial certificate issuance:

- **Identity:** The applicant appears in-person before an RA Officer or TA and presents either a valid Personal Identity Verification (PIV) card issued in compliance with *Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors* [FIPS 201] or two forms of identity source documents in original form. Valid identity source documents are listed in *OMB No. 1615-004, Form I-9, Employment Eligibility Verification* [FORM I-9]. At least one document must be a valid State or Federal government-issued picture identification (ID). For DoD, the PIV Card is the Common Access Card (CAC).

- The RA Officer or TA visually inspects the identification documents and authenticates them as being genuine and unaltered. In addition, the RA Officer or TA electronically verifies the authenticity of the source document, when such services are offered by the issuer of the source document. When electronic verification is not offered, the RA Officer or TA uses other available tools to authenticate the source and integrity of the identity source documents.
- **Citizenship:** For Name certificates where the Subscriber has an EDIPI, citizenship is provided by Secret-Authentication Data Repository (S-ADR). Otherwise, citizenship is verified by checking the clearance records at the local security office.
- **Clearance:** The RA Officer or TA ensures that the applicant possesses a minimum of a current SECRET clearance. The clearance is determined through an authoritative source (e.g., security database). If local policy/process guarantees that having a network login account on a U.S. SECRET network guarantees a current SECRET clearance and that if the person leaves the organization or has their clearance rescinded, the account is immediately deactivated, the RA Officer or TA may rely on the account verification for this check.
- **Account:** The RA Officer or TA ensures the applicant possesses a network login account on an accredited U.S. SECRET level information system or network or the application for PKI certificates is part of the enrollment process for obtaining a network login account on an accredited U.S. SECRET level information system or network. This is done by checking with a local System Administrator known to the RA Officer or TA.
- **Email:** For email address information asserted in a certificate, the RA Officer or TA ensures the validity of the email address provided by checking with a local System Administrator known to the RA Officer or TA.
- **System Administrator Position Designation:** For Name certificates that assert the Personnel Category Code (PCC) of "ADM" in the User Principal Name, the RA Officer or TA uses local knowledge to verify that the PKI Sponsor does perform that duty in the local environment.

If the RA Officer/TA obtains information from an individual, it will be in-person, in hard copy with wet signature, or in a digitally signed email using an *id-CNSS-hardware* Name Signature certificate.

The RA Officer or TA signs a DD Form 2842 [DD Form 2842] declaration acknowledging that they have verified the identity and any attributes.

For electronic authentication, see [CAS CPS].

RA Officers and TAs do not participate in electronic requests for issuance, renewal, re-key, or modification of certificates from the Name Subscribers.

3.2.3.2 Authentication for Role Subscribers

The PKI Sponsor accepting the Role certificate will digitally sign [DD FORM 2842]. The individual's identity will be verified using their *id-CNSS-hardware* Name Signature certificate.

The PKI Sponsor sends the request for a Role certificate to the RBAA or CSAA as appropriate. The request contains documentation describing the role, the users of the role, the contact information for transfer of the token and activation data, and, if others will use the Role certificate, the process the PKI Sponsor uses to control access and verify the user's possession of a valid *id-CNSS-hardware* Name certificate. The request is digitally signed using the PKI Sponsor's *id-CNSS-hardware* Name Signature certificate. The RBAA/CSAA verifies the validity of the role and forwards the original email (with signature intact) to the RA Officer in an email digitally signed using the RBAA/CSAA's *id-CNSS-hardware* Name Signature certificate. The CSAA email will state that the request for a certificate is valid, there is a valid need, the PKI Sponsor is the appropriate person to obtain the certificate, the attributes requested are appropriate to the request, and other information required (e.g., CSID) to execute the Subscriber registration. The RA Officer validates the signature on the RBAA/CSAA email. The RA Officer verifies the authority to speak for the organization to as specified in Section 1.3.7.4.

The RA Officer authenticates the identity of the PKI Sponsor and the specified attributes for Role Certificate through the following mechanisms:

- **Role:** The RBAA or CSAA verifies the need for the Role certificate
- **Authority:** The RBAA or CSAA verifies that the PKI Sponsor is authorized to request a Role Certificate
- **Identity:** The RA Officer verifies that the PKI Sponsor possesses a valid NSS PKI issued Name certificate, and that the PKI Sponsor has a process to ensure that each Role Certificate user possesses a valid Name Certificate by reviewing the details in the request.
- **Attributes:** The RA Officer verifies any other attributes asserted by the Role Certificate via organizational processes

The PKI Sponsor is accountable for the private key associated with the Role Certificate, and acknowledges and accepts overall responsibility for the use of the Role Certificate and protection of its associated private key as part of the delivery process (see Section 6.1.2) or during the issuance process (See Section 4.2.1).

The PKI Sponsor follows the process described in the request to ensure that each individual who has access to the private key associated with the Role Certificate at any time possesses a valid NSS PKI Name Certificate. The PKI Sponsor ensures that no individual continues to have access to the private key associated with the Role Certificate after leaving the Role by maintaining direct control of the token except when signed out to an authorized user.

The RA Officer signs the DD Form 2842 returned by the PKI Sponsor verifying the identity and any attributes in accordance with this CPS and [CNSS 1300].

3.2.3.3 Authentication for System or Device Subscribers

The PKI Sponsor provides documentation identifying the System or Device, and any attributes not part of the standard profile (e.g., Globally Unique Identifier (GUID) in a Domain Controller certificate) and the CA Certificate Request Number to the RA Officer in a digitally signed email using the PKI Sponsor's *id-CNSS-hardware* Name Signature certificate. If the PKI Sponsor is a system administrator, the SA Name certificate is used. If the PKI Sponsor sends the digitally signed email to a local TA, the signed email will be included in the TA email to the RA Officer as an attachment. The RA Officer authenticates the identity of the PKI Sponsor and the specified attributes for System or Device Certificate through the following mechanisms:

- **System or Device:** The RA Officer verifies the approved existence of the System or Device by using local knowledge. If the RA Officer is not local, the RA Officer uses a local TA to verify the existence of the system or device.
- **Authority:** The RA Officer verifies the authority of the PKI Sponsor to request a System or Device Certificate by using the fact that the requestor is an SA (based on the digital signature) or by using local knowledge if the PKI Sponsor is not an SA. If the RA Officer cannot verify the authority because of distance, the RA Officer uses a local TA to verify the PKI Sponsor's authority.
- **Identity:** The RA Officer verifies that the PKI Sponsor possesses a valid NSS PKI issued Name Certificate through the digital signature on the request.
- **Attributes:** System administrators are considered the authoritative source for System and Device information within their domain. If the request is digitally signed with an SA Name certificate, the attributes are deemed verified. If the request is not signed using an SA Name certificate, the RA Officer verifies any attributes asserted by the System or Device Certificate based on local knowledge (e.g., the RA Officer verifies that the FQDN is from the appropriate domain). If the RA Officer cannot verify the attribute because of distance, the RA Officer uses a local TA to verify the PKI Sponsor's attributes using local knowledge.

The PKI Sponsor is accountable for the System or Device Certificate, and acknowledges and accepts overall responsibility for the use of the System or Device Certificate and protection of the associated private key. The PKI Sponsor may formally acknowledge the responsibilities in the digitally signed email request, in a signed DD Form 2842 or locally developed form.

The RA Officer or TA sign a declaration acknowledging that they have verified the identity and any attributes in accordance with this policy.

3.2.4 Non-Verified Subscriber Information

The RA Officer verifies all information included in a certificate as specified above.

3.2.5 Validation of Authority

There are no other explicit or implicit authorities beyond those that the RA Officer validates as described in Section 3.2.3. The CAS relies on the RA Officer to perform that validation prior to RA Officer approving the issuance of the certificate.

3.2.6 Criteria for Interoperation

Not applicable.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

For manual Re-Key, see Section 4.7.

3.3.2 Identification and Authentication for Re-Key After Revocation

The initial issuance process is the only method for obtaining new certificates if the current certificate is not valid.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Subscribers or others listed in Section 4.9.2 may submit revocation requests to an RA Officer /TA, who then authenticates the request. The request may be authenticated in one of the following ways:

- Via a digitally signed message (Note that a Subscriber may sign a certificate revocation request using the key suspected of being compromised, and such a request will be considered valid);
- In person via a signed document (another RA Officer or TA may serve as an intermediary who authenticates the request in a face-to-face transaction and uses local knowledge to determine whether the individual is authorized to make a revocation request);
- Using telephone (follow-up with the original signed document or a digitally signed message prior to taking any action), or;
- Using a signed document conveyed via a secure/non-secure fax.

3.5 IDENTIFICATION AND AUTHENTICATION FOR KEY RECOVERY REQUEST

3.5.1 Subscriber Request

For manual recovery, the PKI Sponsor requests recovery of sponsored certificate private keys by sending a digitally signed email to the RA Officer or TA using the PKI Sponsors *id-CNSS-hardware* Name Signature certificate.

3.5.2 Third Party Request

Entities other than PKI Sponsors may request recovery of escrowed key material. Recovery requests from other than the PKI Sponsor are made directly to an RA Officer or to a TA. The RA Officer or TA uses local knowledge to determine the authority of the requestor. The RA Officer or TA may consult with local organization management and/or legal counsel if appropriate.

If the requestor appears in person to make the request, the RA Officer or TA verifies their identity using the process described in Section 3.2.3.1. The requestor may also send the request via email, digitally signed using the requestor's an *id-CNSS-hardware* Name certificate.

If a TA performs the requestor validation, the TA provides the request along with verification of identity and authority to the RA Officer in an email digitally signed with the TA's *id-CNSS-hardware* Name Signature certificate.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

RA Officers use the appropriate RA Officer Name Identity, Signature or Encryption certificate for all communication related to PKI. All TA communications with an RA Officer is digitally signed using the TA's *id-CNSS-hardware* Name Signature certificate. If necessary for privacy or to protect "need to know" (e.g., transfer of activation data), information will be encrypted using the *id-CNSS-software* Name Encryption certificate. RA Officer communication to the CA is authenticated and encrypted using Client-authenticated Transport Layer Security (TLS) using the RA Officer's *id-CNSS-hardware* Name Identity certificate and the CA Device certificate. Subscribers authenticate to the Token Processing System (TPS) component of the DoD NSS Subordinate CAS using the UID and one time password provided by the RA Officer. The Subscriber authentication occurs within a server authenticated TLS session.

4.1.1 Who Can Submit a Certificate Application

Either PKI Sponsor is present when the keys are generated and the certificate request is submitted to the CA or the keys are generated and the request sent to the CA by the RA Officer on behalf of the Subscriber. If the PKI Sponsor is present when the keys are generated, the PKI Sponsor is considered to be in possession of the private key.

The System or Device PKI Sponsor generates a public/private key pair and formats that into a PKCS#10 certificate request using their System or Device application software and submits the request via a secure (TLS protected) Web session.

For RA Officer or Subscriber interaction with the CA during the certificate issuance process, see [CAS CPS].

4.1.2 Enrollment Process and Responsibilities

The generation of RA Officer certificates occurs in the same manner as for Subscriber certificates except that the DN is of the RA/LRA/NVO form.

For certificates with the RA name form: RA Officers with Revocation and/or recovery privileges are nominated by a CC/S/A official (identified separately) to DISA in a signed memorandum - electronic transmission with digital signature using a *id-CNSS-hardware* Name, *id-US-dod-mediumHardware* or *id-US-dod-mediumHardware-2048* certificate is permitted. An example nomination memorandum is included at Appendix D. At initial RA Officer training, the RA Officer conducting the training or another RA Officer authenticates the candidate RA Officer face-to-face in accordance with the requirements of Section 3.2.3.1.

For certificates with the LRA or NVO name form: LRA/NVOs are nominated by the local command to an RA Officer in a signed memorandum - electronic transmission with digital signature using a *id-CNSS-hardware* Name, *id-US-dod-mediumHardware* or *id-US-dod-mediumHardware-2048* certificate is permitted. An example nomination memorandum is included at Appendix E. At initial LRA/NVO training, the RA Officer conducting the training or another RA Officer authenticates the candidate LRA/NVO face-to-face in accordance with the requirements of Section 3.2.3.1. If the LRA functioned as an LRA under the SIPRNET Pilot, that fact is stated in the nomination memorandum and these LRAs may be authenticated by an RA Officer, or TA as is done for any Subscriber. Subsequent face to face authentication of an existing LRA/NVO for issuance of new certificates with the same DN may be done by any RA Officer, LRA, NVO or TA as for any Subscriber. While a TA may authenticate an LRA/NVO, this should only be done if no RA Officer is available due to operational constraints (e.g., remote location). The RA Officer performing the LRA/NVO registration documents the need to use a TA in the RA Officer log.

Once candidate RA Officer /LRA/NVO has their RA Officer /LRA/NVO certificates, the candidate forwards a copy to the registering RA Officer. The registering RA Officer verifies the certificate against the registration information and emails the new RA Officer /LRA/NVO certificate to the CA Administrator (CAA) to add them to the appropriate privilege groups on the CAS.

For Hardware Subscriber Name certificates:

Once the RA Officer has received and verified all the required information, the RA Officer registers the subscriber with TPS by entering all required data into the interface provided. TPS generates Certificate Registration Instructions (CRI) containing a User Identification and one-time 16-character password.

If the PKI Sponsor is present at the certificate generation:

After the Subscriber signs the acknowledgement of responsibilities form ([DD FORM 2841] for RA Officers or [DD Form 2842] for other Subscribers), the RA Officer or TA provides the CRI and a token to the PKI Sponsor. Signatures on the acknowledgment of responsibilities form may use digital signatures using a valid *id-CNSS-hardware* Name Signature certificate.

The PKI Sponsor uses the token and CRI to authenticate to TPS and generate the certificate request as specified in [CAS CPS].

If a TA does the identity proofing, the TA forwards the acknowledgement of responsibilities form to the RA Officer. If in hard copy, the TA faxes or sends a scanned copy to the RA Officer immediately and forwards the paper copy via US Mail.

If a hard copy [DD FORM 2842] is transmitted, when the RA Officer receives the original hard copy of the Certificate of Acceptance and Acknowledgement of Responsibilities, the faxed/emailed copy may be destroyed.

If the RA Officer generates the certificates on behalf of the Subscriber:

The RA Officer performs the PKI Sponsor functions associated with generating the certificate request as specified in [CAS CPS]. The RA Officer immediately secures the keyed token and PIN in separate containers. PIN is classified SECRET and will be controlled accordingly. The token and PIN are provided to the PKI Sponsor as specified in Section 6.1.2.

For software Subscriber Name Certificates:

The RA Officer registers the Subscriber with the LRA Server, where a UID and one-time 16-character password are generated. After the Subscriber signs the acknowledgement of responsibilities form [DD Form 2842], the RA Officer or TA provides the CRI to the PKI

Sponsor. Signatures on the acknowledgment of responsibilities form may use digital signatures using a valid *id-CNSS-hardware* Name Signature certificate.

The PKI Sponsor uses the CRI to authenticate to the CA and generate the certificate request as specified in [CAS CPS].

If a TA does the identity proofing, the TA forwards the acknowledgement of responsibilities form to the RA Officer. If in hard copy, the TA faxes or sends a scanned copy to the RA Officer immediately and forwards the paper copy via US Mail.

If a hard copy [DD FORM 2842] is transmitted, when the RA Officer receives the original hard copy of the Certificate of Acceptance and Acknowledgement of Responsibilities, the faxed/emailed copy may be destroyed.

For Role Certificates[2]: The PKI Sponsor will submit a request to the RBAA or CSAA, as appropriate, who will verify and forward the request to the RA Officer as specified in Section 3.2.3.2. The RA Officer will verify that it has received a signed designation for the RBAA/CSAA. This verification will include the verification of digital signature if the RA Officer received an electronic copy of the RBAA/CSAA designation. The RA Officer will request the certificate from the CA on behalf of the applicant and notify the applicant that the request has been made and provide the PKI Sponsor with the CRI in accordance with Section **Error! Reference source not found.**, once all verification and checks have been completed.

For System and Device Certificates: The PKI Sponsor (normally an SA) forwards the request (including the identifying information and other attributes) along with the CA request number to the RA Officer as specified in Section 3.2.3.3. When an RA Officer receives notification that a System or Device certificate request is in-process, the RA Officer uses the request number to confirm that the request information matches the request posted on the CA server.

4.2 CERTIFICATE APPLICATION PROCESS

4.2.1 Performing Identification and Authentication Functions

If the RA Officer or TA uses local knowledge to verify information prior to certificate approval, the local knowledge is obtained by establishing a relationship with offices that have authority to assign information or attributes.

For Name Subscribers:

The RA Officer or TA performs authentication as described in Section 3.2.3.1. The RA Officer ensures that all information related to the Subscriber to be included in the certificate is accurate prior to providing the PKI Sponsor with the token and CRI. If the PKI Sponsor has an EDIPI, the person verifying the identity verifies the PKI Sponsor’s EDIPI by inspection of a CAC, a document digitally signed using the private key from the CAC or other information provided by

[2] When a shared encryption capability is the primary reason for the group certificate, an identity certificate must be created to generate the encryption certificate, but serves no further purpose and may be destroyed, but not revoked. A signing certificate need not be generated at all. Microsoft based systems can use the “SupressNameChecks” policy that will allow users to select their existing Name ID or Signing Certificate on their personal CNSS Token for signature from the group mail-box and thus maintain individual non-repudiation without the need to generate unique signing certificates for each member of the group.

the PKI Sponsor. The RA Officer verifies that the identity information provided by the PKI Sponsor matches that displayed by S-ADR for the EDIPI.

If the RA Officer uses a TA to perform any data verification, the TA verifies the data prior to submitting it to the RA Officer. The data is transmitted to the RA Officer in an email digitally signed with the TA's Signature *id-CNSS-hardware* Name certificate. The RA Officer validates the emails digital signature and verifies it is from the TA.

The RA Officer will print, on a printer on the same subnet, the CRI generated by TPS or the LRA Server for each Subscriber that includes:

- A unique user identification
- A one-time password

If the RA Officer is going to generate the keys and certificates for the Subscriber, the RA Officer retains the CRI until it has been used and then destroys it.

If the PKI Sponsor will be present at certificate generation, the RA Officer delivers the CRI form in person directly to the PKI Sponsor, authenticating their identity in accordance with the requirements of Section 3.2.3.1. or the RA Officer delivers the CRI to a TA using one of the methods detailed below.

- The RA Officer may deliver the CRI form(s) in person directly to the TA; or,
- The RA Officer may send the CRI form, in its entirety, to the TA in a signed and encrypted S/MIME message on SIPRNET.

The RA Officer or TA, prior to providing the CRI, keyed token and PIN, or P12 file and password to the PKI Sponsor, will perform the identity proofing required by Section 3.2.3.1 and have the Subscriber sign the Certificate of Acceptance and Acknowledgement of Responsibilities that includes:

- A listing of their responsibilities as a Subscriber;
- Instructions regarding contacting the RA Officer in the event of a suspected compromise.

If the PKI Sponsor is using the CRI to directly interact with the CA, the person performing authentication instructs the PKI Sponsor to contact the RA Officer or TA if the one time password does not work. The TA informs the RA Officer. Upon being so informed, the RA Officer investigates whether or not the one time password has been used and a certificate created in the subscriber's name. If the CRI has been used to issue certificates in the subscriber's name, the RA Officer revokes all issued certificate (LRA/TA requests the RA Officer to revoke the certificates) and request that the PKI Sponsor's Security Officer investigate. If the Subscriber still requires a certificate, the RA Officer generates a new CRI. The new CRI is delivered to the PKI Sponsor using the same procedures (including identity checking and acknowledgement of responsibilities) as specified above.

For Role certificates:

A Role Based certificate is tied specifically to the PKI Sponsor who is identified in the Subject Alternative Name field of the certificate. The PKI Sponsor is responsible for control and use of the certificate and associated private key. The PKI Sponsor may authorize another to use the Role certificate. The PKI Sponsor maintains signature records of who used the certificate and when. Ultimately, should an issue arise, the PKI Sponsor issued the certificate will be the one contacted for resolution.

The PKI Sponsor performs the following:

- Send an email digitally signed using the PKI Sponsor's *id-CNSS-hardware* Name Signature to the RBAA/CSAA, copy to the RA Officer, requesting authorization to obtain a Role certificate. If it is for a Code Signing certificate, the PKI Sponsor acknowledges that the Code Signing certificate private key requested may only be used for three years.

The RBAA/CSAA will perform the following:

- Validate the PKI Sponsor's request, to include verification of the PKI Sponsor's identity and need for the requested certificate;
- Submit a signed e-mail to the RA Officer validating that the certificate and contact information in the PKI Sponsor's request for issuance of a Role Certificate is correct, that the RBAA/CSAA approves the issuance of the Role Certificate and, if necessary, provides any information not in the PKI Sponsor's request required by the RA Officer to complete the request as specified in Section 3.2.3.2. This e-mail is digitally signed with the RBAA/CSAA's *id-CNSS-hardware* Name Signature certificate. The information the RA Officer needs to complete the request:
    - Information on attributes necessary to complete the certificate request
    - PKI Sponsor's Organizational Information and, for a Code Signing Certificate, the assigned CSID for the CN
    - Authorized PKI Sponsor's Contact Information

The RA Officer will conduct the following steps:

- Verify that they have received a digitally signed e-mail from the RBAA/CSAA for the code signer; verify that the e-mail is signed by an approved RBAA/CSAA; and, that the e-mail was signed using acceptable PKI credentials and perform identity verification and authentication as specified in Section 3.2.3.2
- Verify that the following DNs are identical: DN for the PKI Sponsor in their e-mail to the RBAA/CSAA and the DN of the person mentioned in the e-mail from the RBAA/CSAA

For Hardware Role Certificates (Note: Code Signing Certificates are only issued in hardware format):

- The RA Officer enters all required data into the TPS Role Certificate interface
- The RA Officer will print, to a file (e.g., PDF) or hardcopy on a printer on the same subnet, the CRI generated by TPS for the Role that includes:
    - A unique user identification
    - A one-time password
- The RA Officer formats a new token using the appropriate Phone Home URL.
- If the RA Officer is going to generate the keys and certificates for the Subscriber, the RA Officer retains the CRI until it has been used and then destroys it, performs enrollment and sends the token and pin as specified in Section 6.1.2.

- If the PKI Sponsor will be present at certificate generation, the RA Officer notifies the PKI Sponsor that the request has been processed and approved and request that the PKI Sponsor execute a DD Form 2842. The PKI Sponsor digitally signs the DD Form 2842 using the PKI Sponsor's *id-CNSS-hardware* Name Signature certificate and returns it to the RA Officer in a digitally signed email. The RA Officer send the CRI form to the PKI Sponsor in a digitally signed email, encrypted using the PKI Sponsor's *id-CNSS-software* Encryption certificate. The RA Officer sends the token to the PKI Sponsor as specified in Section 6.2.1.

For Software Role Certificates:

- The RA Officer enters all required data into the LRA Server Certificate interface
- The RA Officer will print, to a file (e.g., PDF) or hardcopy on a printer on the same subnet, the CRI generated by LRA Server for the Role that includes:
    - A unique user identification
    - A one-time password
- If the RA Officer is going to generate the keys and certificates for the Subscriber, the RA Officer retains the CRI until it has been used and then destroys it, performs enrollment and sends the P12 file and the password as specified in Section 6.1.2.
- If the PKI Sponsor will be present at certificate generation, the RA Officer notifies the PKI Sponsor that the request has been processed and approved and request that the PKI Sponsor execute a DD Form 2842. The PKI Sponsor digitally signs the DD Form 2842 using the PKI Sponsor's *id-CNSS-hardware* Name Signature certificate and returns it to the RA Officer in a digitally signed email. The RA Officer send the CRI form to the PKI Sponsor in a digitally signed email, encrypted using the PKI Sponsor's *id-CNSS-software* Encryption certificate.

For System or Device Certificates: See Section 3.2.3.3.

4.2.2 Approval or Rejection of Certificate Applications

A certificate application is not considered accepted until the CA has acted on the application and issued a certificate. If, for any reason, the certificate request is rejected prior to completion of the process, the RA Officer will inform the PKI Sponsor of the reason for the rejection. If the certificate is still required, the PKI Sponsor will make the appropriate corrections to the data submitted and resubmit. The RA Officer or TA will, when requested, provide guidance to the PKI Sponsor.

4.2.2.1 Name Certificate Application

The RA Officer approves the issuance of the certificate when enrolling the Name Subscriber as described in Section 4.2.1.

4.2.2.2 Role Certificate Application

The RA Officer approves issuance of the certificate when enrolling the Role Subscriber as described in Section 4.2.1..

4.2.2.3 System or Device Certificate Application

When an RA Officer receives notification, either directly or via another RA Officer or TA, that a System or Device certificate request is in process, the RA Officer uses the request number to confirm that the request information matches the request posted on the CA server. The RA Officer ensures the DN structure and other information in the certificate conforms to the requirements of Sections 3.1.2.4 or 3.1.2.5, and, if not, makes corrections as permitted by the CA interface to insure proper format and features are included in the certificate to match the customers requirement. If the RA Officer is satisfied, the RA Officer will approve the certificate for up to three years, and send an e-mail notification to the PKI sponsor that the certificate can be obtained from the CA server.

4.2.3 Time to Process Certificate Applications

For certificates issued by the CA based on input of a CRI, the CA rejects the CRI if it was generated more than 30 days prior to entry.

If the 30 day limit passes for any reason, the RA Officer/TA will redo the authentication of the PKI Sponsor prior to providing an updated CRI.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

Not applicable.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

After the CA issues the certificate, the RA Officer notifies the Subscriber or the sponsor if the RA Officer manually approves certificate issuance. Otherwise, the Subscriber is considered to have been notified when the certificate is provided directly to the Subscriber.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

The PKI Sponsor’s signature (hand written or digital) on the [DD FORM 2841] or [DD FORM 2842] or other appropriate acknowledgement of responsibilities obtained during the certificate request process is deemed as the acceptance of the certificate**.**

4.4.2 Publication of the Certificate by the CA

Not applicable.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber should not use the signature private key after the associated certificate has been revoked or has expired. The Subscriber may continue to use the decryption private key solely to decrypt previously encrypted information after the associated certificate has been revoked or has expired. The use of the private key is further limited in accordance with the key usage extension in the certificate. If the extended key usage extension is present and implies any limitation on the use of the private key, those constraints are also observed.

4.5.2 Relying Party Public Key and Certificate Usage

A Relying Party should only use a public key for the purposes indicated in the certificate *Key Usage* extension. Relying Parties should not use expired or revoked encryption certificates. If the *Extended Key Usage* extension is present and implies any limitation on the use of the certificate, those constraints should also be followed.

4.6 CERTIFICATE RENEWAL

Not applicable.

4.7 CERTIFICATE RE-KEY

The RA Officer has no part in automated Re-key.

The RA Officer may assist in manual re-key of Name and Role Certificates for Subscribers as specified below.

System or Device Certificates issued via the manual process described in this RPS are rekeyed using the initial issuance process.

4.7.1 Circumstances for Certificate Re-Key

A certificate may be re-keyed if all of the following are true:

- The certificate has not reached the end of its validity period;
- The certificate has not been revoked;
- The name and other information in the certificate is still correct;
- The identity proofing of the PKI Sponsor is current; and,
- The RA Officer re-validates proof of possession of the old Signature private key by the PKI Sponsor by validating the email signature.

4.7.2 Who May Request Re-Key

The PKI Sponsor requests re-key of a Subscriber certificate.

4.7.3 Processing Certificate Re-Key Requests

The PKI Sponsor sends an email, digitally signed with the Subscriber's *id-CNSS-hardware Signature* certificate to the TA/RA Officer that processed their initial certificate request. If the PKI Sponsor does not know the identity of the RA Officer/TA, the PKI Sponsor is directed to the initial registration process. If a TA receives the request from the PKI Sponsor, the TA forwards that request to the RA Officer that performed the initial subscriber registration in a way that does not invalidate the PKI Sponsor's signature.

The RA Officer performs the following steps:

- Validate the certificate used by the PKI Sponsor to sign the request and that the certificate has not been used for a previous rekey request:
- Obtain the [DD Form 2842] of the PKI Sponsor and verify that it has been less than 3 years since the PKI Sponsor did a face to face authentication;
- For Hardware Name Certificates, authenticate to TPS and uses the PKI Sponsor's EDIPI to view the record from S-ADR;
- For Software Name Certificates, authenticate to the LRA Server and re-enroll the PKI Sponsor using the information in the current certificate;
- For Hardware Role Certificates, authenticate to TPS and view the Role Certificate record;
- For Software Role Certificates, authenticate to the LRA Server and re-enroll the PKI Sponsor using the information in the current certificate;
- Obtain a new CRI for the PKI Sponsor; and,
- Send the CRI to the PKI Sponsor encrypted using the *id-CNSS-software* certificate associated with the Signature certificate used to sign the request.
- For software certificates or if the Subscriber hardware token does not destroy the original private keys in the process of generating the rekeyed certificate, the RA Officer records the certificate used to authenticate for the rekey.

If the certificate is not valid, was previously used to authenticate for rekey of a Name Certificate, the face-to-face exceeds 3 years for the Subscriber Certificate, or the information in TPS and the original certificate do not match, the RA Officer stops the process and directs the PKI Sponsor to use the initial registration process to obtain a new set of certificates.

Upon receipt of the new CRI, the PKI Sponsor uses the token and CRI to authenticate to TPS or the CRI and a web browser to authenticate to the CA and generate the certificate request as specified in [CAS CPS].

4.7.4 Notification of New Certificate Issuance to Subscriber

The PKI Sponsor receives the new certificates as a result of the certificate issuance process.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The PKI Sponsor's use of the CRI to authenticate to the TPS to obtain new certificates and subsequent failure to object to the issued certificate or its contents constitute acceptance of the certificate.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The CA posts the encryption certificate in the same manner as for any other certificate set.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.8 CERTIFICATE MODIFICATION

Not applicable.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

The RA Officer only accepts revocation requests that are either digitally signed with an NSS certificate issued at the same or stronger assurance level, a request that is submitted in person with identity proofing as specified in Section 3.2.3.1 or a document with a handwritten signature. The CAS only accepts authentication requests from the RA Officer which authenticates using client authenticated TLS using the RA Officer *id-CNSS-hardware* Name Identity certificate.

4.9.1 Circumstances for Revocation

The RA Officer evaluates each request for revocation to determine if it is reasonable to state that the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Circumstances that invalidate the binding include the following:

- Identifying information or affiliation components of any names in the certificate become invalid;
- Information not included in the certificate but required for the issuance of the certificate becomes permanently invalid (e.g., a PKI Sponsor's U.S. SECRET network account is deactivated and the PKI Sponsor is not known to be transferring to another organization where the PKI Sponsor will have a U.S. SECRET network account (see Section 4.9.13));
- Privilege attributes asserted in the certificate are no longer accurate;
- The PKI Sponsor can be shown to have violated the stipulations of the PKI Sponsor agreement;
- The private key is suspected of compromise;
- For Name Certificates, the individual named in the certificate is no longer authorized to hold the certificate; and,
- Unlocking the token in an unclassified machine.

If the RA Officer determines that the binding is likely to be invalid, the RA Officer accesses the appropriate CA and marks the certificate for revocation.

If the PKI Sponsor or other authorized party provides appropriate justification in an authenticated manner, the RA Officer accesses the appropriate CA and marks the certificate for revocation.

If a Subscriber cryptographic module is suspected to have been lost, the PKI sponsor reports that immediately to an RA Officer /LRA or TA. The LRA/TA forwards the report to an RA Officer. The RA Officer immediately accesses the appropriate CA(s) and marks all certificates associated with the module as suspended pending investigation. If loss of control is confirmed, the RA Officer accesses the appropriate CA(s) and changes all certificates associated with the module to revoked for reason of compromise. PKI Sponsors are informed to not use a token which has potentially been compromised. If the cryptographic module is reacquired, it is destroyed as specified in Section 6.2.10.

4.9.2 Who Can Request a Revocation

The RA Officer can request the revocation of a Subscriber's certificate on behalf of any of the following:

- The PKI Sponsor;
- The Subscriber’s IAO or personnel security officer; or,
- CC/S/A Information Assurance or network defense personnel.

Requests may be sent directly to the RA Officer or via an RA Officer/TA.

The RA Officer uses local knowledge to determine whether the individual is authorized to make a revocation request. If the requestor is not local to the RA Officer, the RA Officer requests the assistance of another RA Officer or TA who is local to the requestor to verify the authority of the requestor.

4.9.3 Procedure for Revocation Request

The requestor provides the RA Officer with sufficient information to allow the RA Officer to determine if there is appropriate justification to revoke the certificate. The RA Officer will review all revocation requests to ensure that the revocation requests are legitimate; the request identifies the specific certificate(s) or the/token containing the certificates to be revoked and the reason for revocation. If received electronically, it is digitally signed using a certificate of at least the same assurance level as the certificate to be revoked. The RA Officer validates the signature prior to taking any action on the request. If received manually, the request is signed by the requestor.

If the revocation is being requested for reason of key compromise or suspected fraudulent use, then the originator’s and RA Officer’s revocation request so indicates.

The RA Officer will review all revocation requests to ensure that the revocation requests are legitimate and will then approve the revocation of the certificate, as follows:

- Authenticate revocation request, as defined in Section 3.4 of this RPS;

- Establish a TLS connection to the CA or TPS;
- Authenticate to the appropriate CA (for certificates not issued through TPS) or TPS (for token based certificates) using the RA Officer's PKI credential; Use the web based revocation form to provide the information necessary to identify the token containing the certificates to be revoked as described in [CAS CPS]; and,
- For bulk revocation, use the search function to identify the set of tokens to be revoked, verify the search results only includes the tokens and certificates to be revoked as described in [CAS CPS].

If the RA Officer receives a request for revocation from other than a party listed in Section 4.9.2, the RA Officer directs the person submitting the request to the PKI Sponsor's IAO or personnel security officer to verify the authenticity of the request. If the PKI Sponsor's IAO or personnel security officer agrees there is reason for revocation, the IAO or personnel security officer sends an authenticated request to the RA Officer for processing.

For hardware certificates, the RA Officer revokes all certificates when the token is turned in or the RA Officer is notified that the Subscriber no longer has a requirement regardless of whether the token is turned in or not. If the token is not turned in, or the token is not protected from malicious activity prior to zeroization, the reason code for the revocation is "compromise." If it is determined that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, the RA Officer will review certificate request records and work with the CAA to attempt to determine all certificates directly or indirectly chaining back to that compromised key and revoke those.

As part of the out processing, all persons who have NSS hardware tokens are required to turn them in to their local security office unless they are approved to take the token with them to a follow on assignment (see Section 4.9.13.3). The local security office notifies the RA Officer of all out processing individuals who had SIPRNet accounts and whether the token was turned in.

4.9.4 Revocation Request Grace Period

The RA Officer completes processing of all revocation requests immediately upon receipt.

4.9.5 Time within Which CA Must Process the Revocation Request

The RA Officer completes processing of all revocation requests immediately upon receipt.

4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party. Revocation data should be obtained from an authoritative source, such as a CRL or an authoritative CSS as defined in [CNSSI 1300].

If it is temporarily infeasible to obtain revocation information from an authoritative source, then the Relying Party should either reject use of the certificate or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy.

The RA Officer validates all certificates either using CRLs or an authoritative CSS. The RA Officer will ensure that the CRL used to check the certificate has not reached its Next Update.

4.9.7 CRL Issuance Frequency

Not applicable.

4.9.8 Maximum Latency for CRLs

Not applicable.

4.9.9 On-line Revocation/Status Checking Availability

Not applicable.

4.9.10 On-line Revocation Checking Requirements

The RA Officer validates all certificates either using CRLs or an authoritative CSS.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Related to Key Compromise

See 5.7.1 for incident and compromise handling and Section 5.7.3 for entity private key compromise procedures. See Section 4.9.3 for revocation procedures.

4.9.13 Certificate Suspension and Restoration

4.9.13.1 Circumstances for Suspension

When there is reason to believe that the binding between the subject and the subject’s public key defined within a certificate is not currently valid (e.g., the PKI Sponsor is reassigned to another organization and does not have an account on a U.S. SECRET network during the transition), or there may be reason to question the security of the private key, but additional research is necessary to determine the status fully, the person informing the RA Officer of the need for revocation may request suspension instead. See [CNSS 1300] for examples.

4.9.13.2 Who Can Request Suspension

All persons authorized to request revocation may request suspension.

4.9.13.3 Procedure for Suspension Request

Except for suspension due to reassignment, the requestor uses the same procedures as specified for revocation. In addition to the information required for revocation, the requestor provides a time when it is expected that a final determination may be made.

When a PKI Sponsor is being reassigned within the organization (attributes do not change) and temporarily will not have an account on a U.S. SECRET network:

When notified of pending reassignment, the PKI Sponsor or other authorized person contacts the unit Information Assurance Manager (IAM) or other person authorized to request suspension of certificates for the unit (referred to as the requestor);

The requestor provides the RA Officer/TA with the gaining organization information (e.g., a copy of the reassignment orders), the expected date that the U.S. SECRET Network account will be closed, a copy of the PKI Sponsor's Name Identity certificate and the expected date of restoration. Documentation may be provided in person or via digitally signed email using the requestor's Name Hardware certificate;

The RA Officer/TA validates the requestor's identity;

If it is a TA, the TA forwards all information to the RA Officer;

On the requested date, the RA Officer accesses TPS and suspends all of the certificates associated with the subscriber token.

Note: The PKI Sponsor may hand carry the suspended token to the new organization or request that the RA Officer/TA send it to the gaining organization RA Officer/TA using the procedures specified in Section 6.1.2.

4.9.13.4 Limits on Suspension Period

The RA Officer maintains a log of all suspended certificates indicating the expected time to resolve or restore. If the RA Officer has any active suspended certificates, the RA Officer reviews that log every business day. The RA Officer revokes any certificate that is beyond its expected time to resolve or restore. The requestor may, prior to that time, submit an authenticated request to extend the time to resolve or restore.

4.9.13.5 Circumstances for Restoration

For a suspended certificate, once the issue that resulted in the suspension request has been resolved and it is determined that the binding between the subject and the subject's public key defined within a certificate is still valid and there was no compromise of the private key, the certificate may be restored once the RA Officer has performed the steps below. See [CNSS 1300] for examples.

4.9.13.6 Who Can Request Restoration

Except for suspension due to reassignment, the RA Officer may accept restoration requests from the individual who made the initial suspension request except a PKI Sponsor for the PKI Sponsor's own Name Certificate, or, with sufficient justification, from other individuals. The request is signed with a wet signature if the request is submitted in writing or using *id-CNSS-hardware* Name certificate if submitted electronically.

For restoration of certificates suspended due to reassignment, the RA Officer may accept a restoration request from the PKI Sponsor.

4.9.13.7 Procedure for Restoration Request

Except for suspension due to reassignment, the request for a restoration identifies the certificate to be restored, and provides the reason for restoration. Prior to approving a certificate restoration, the RA Officer validates the restoration request to include:

- Ensuring the request has appropriate justification;

- Authenticating the identity of the requestor; and,
- Verifying the requestor's authority to request restoration

The RA Officer does not accept restoration requests from the PKI Sponsor for the PKI Sponsor's own Name Certificate. If the PKI Sponsor requests restoration, the RA Officer informs the PKI Sponsor that the request needs to be sent from someone in the PKI Sponsor's chain of command. For other requests, the RA Officer only accepts digitally signed restoration requests signed using the requestor's *id-CNSS-hardware* Name Signature certificate.

For Name certificates, the RA Officer only accepts restoration requests from the PKI Sponsor's manager, supervisor, or superior officer. The manager, supervisor, or superior officer is responsible for determining if restoration or revocation is warranted and informs the RA Officer of that determination. The RA Officer uses local knowledge (directly, or through a TA) to determine that the requestor holds an appropriate position to make the determination.

For suspension due to reassignment:

Upon arrival, the PKI Sponsor notifies the gaining organization IAM or other person authorized to request restoration that the PKI Sponsor has suspended certificates. The requestor notifies the RA Officer/TA, providing the expected date when the U.S. SECRET network account will be activated;

The PKI Sponsor appears in person before the RA Officer/TA. The RA Officer/TA verifies the PKI Sponsor's identity as specified in Section 3.2.3.1 and verifies that the identity matches the identity in the certificates to be restored;

Prior to restoring the certificates, the RA Officer/TA verifies the security clearance, account activation and email address as specified in Section 3.2.3.1;

If it is a local TA, the TA notifies the RA Officer of the need to restore the Name certificates and the RA Officer verifies that the TA has checked the identity, clearance, account activation and email address;

The RA Officer accesses TPS and restores the certificates.

Once the certificate is revoked, the RA Officer rejects all requests to restore it.

4.10 CERTIFICATE STATUS SERVICES

Not applicable.

4.10.1 Operational Characteristics

Not applicable.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

Subscription is synonymous with the certificate validity period. The subscription ends when the certificate expires or is revoked.

4.12 KEY ESCROW AND RECOVERY

The NSS PKI supports key escrow and recovery for private keys associated with encryption certificates. The NSS PKI does not support key recovery using key encapsulation techniques.

4.12.1 Key Escrow

4.12.1.1 Circumstances for Key Escrow

Encryption certificate private keys are escrowed as part of the key generation/certificate request process. Those are the only private keys that are escrowed.

4.12.1.2 Escrowing Keys

Not applicable.

4.12.1.3 Notification of Key Escrow to Subscriber

The Subscriber [DD FORM 2842] advises the PKI sponsor that private keys associated with their encryption certificates are escrowed by the PKI.

4.12.2 Key Recovery

The DoD implementation does not issue *id-CNSS-hardware* OID encryption certificates.

For *id-CNSS-software* OID encryption certificates, the RA Officer interacts with the DRM through the TPS interface. The RA Officer may specify recovery to Token if the associated certificate has been lost or destroyed. All other private keys are recovered in software. The DRM provides the key to the TPS as described in [CAS CPS]. For token recovery, TPS produces a CRI which is used to extract the private key from the DRM and insert it into the Token. For software recovery, the private key and certificate are provided in a PKCS 12 file. Keyed Tokens, P12 files and password are distributed to the requestor as specified in Section 6.1.2 for distribution private keys.

4.12.2.1 Circumstances for Key Recovery

Escrowed keys may be recovered to support the recovery of encrypted data for business, law enforcement or other requirements. In general, escrowed keys are recovered for the following purposes:

- The original copy of the escrowed key has been lost or damaged and the Subscriber cannot access data encrypted with the corresponding public key;
- The certificate is to be re-keyed and the earlier issued private keys are recovered to be included on the token containing the re-keyed certificate; and,
- An authorized third party (other than the PKI Sponsor) requires access to data encrypted with the corresponding public key.

4.12.2.2 Who May Request Key Recovery

PKI Sponsors may request recovery of their own escrowed keys. RA Officers may request initiation of the recovery of escrowed keys as part of the re-key process. Key recovery may also be requested by the following third parties:

- PKI Sponsor's manager, supervisor, or superior officers;
- Law enforcement or counterintelligence agents;
- Agents of U.S. Federal Courts; and,
- Any person or organization authorized by the NSS PKI PMA or ANMA via an authenticated communication.

4.12.2.3 Processing Key Recovery Requests

The RA Officer only accepts requests signed with a wet signature if the request is submitted in writing or using *id-CNSS-hardware* Name Signature certificate if submitted electronically. Requests may be submitted directly to the RA Officer or through a local TA.

For all requests processed through the RA Officer, the RA Officer or TA validates the identity of the requestor, and RA Officer determines the authority of the requestor to recover the escrowed key using local knowledge (directly, or through the TA). The RA Officer or TA confers with organization management and/or legal counsel, as appropriate.

If a TA receives the request, the TA validates the authority of the individual using local knowledge and forwards the request (in a format that allows the RA Officer to validate the requestor's signature) via a digitally signed email to the RA Officer. The TA states the basis for accepting the requestor's authority. The RA Officer authenticates the information in the request.

For all manual key recovery operations, once the RA Officer has completed validating the recovery request, the RA Officer initiates the key recovery process, which requires the participation of two RA Officers, as follows:

The original RA Officer (called the 1st RA Officer) provides all information to a 2nd RA Officer at the same location. The 2nd RA Officer verifies the information using the same process as the 1st RA Officer;

The 1st RA Officer obtains a signed acknowledgement of responsibilities from the requestor stating that the Third Party requestor agrees to be bound, by legal and policy means, to the key protection and other provisions of this CP, including use of activation data that complies with Section 6.4.1;

Once both RA Officer s are satisfied, the 1st RA Officer authenticates to the TPS using the 1st RA Officer's *id-CNSS-hardware* RA Officer certificate;

After the 1st RA Officer has successfully authenticated, the 1st RA Officer identifies the certificate for the key to be recovered to the system and, specifies whether the key will be recovered in software or to a token (TPS will provide options based on policy OID and token state);

The 1st RA Officer then provides the request identification information to the 2nd RA Officer.

The 2nd RA Officer authenticates to the TPS using the 2nd RA Officer's *id-CNSS-hardware* RA Officer certificate. The 2nd RA Officer ensures that the specific request information matches the documentation provided and approves the 1st RA Officer to recover the key;

For recovery to software:

The 1st RA Officer receives the system generated password used to encryp the private key into the PKCS12 file;

The 2nd RA Officer receives and accounts for PKCS#12 file containing the certificate and private key; and,

The RA Officers transmit the recovered key and password to the requestor using the process described in Sections 6.1.2 and 6.2.6.

For recovery to a Token:

Each RA Officer prints the CRI presented by the system. Each CRI contains half of the authentication information required to recover the key to the token.

The 1st RA Officer formats a token with the Key Recovery phone home URL;

If the requestor will recover the key directly, the 1st RA Officer sends the Token to the requestor as specified in section 6.2.1. Each RA Officer forwards the partial password CRI to the requestor in a digitally signed and encrypted email. The requestor uses the Token and the user name and combined CRI password to obtain the Private Key;

If the RA Officers will recover the key to the Token, the two RA Officers work together, each providing half of the CRI password to obtain the Key. The 1st RA Officer maintains control of the Token and the 2nd RA Officer inputs and maintains control the PIN for the Token. Token and PIN are sent to the Requestor as specified in Section 6.1.2.

4.12.2.4 Notification of Key Recovery to Subscriber

For manual recovery, the RA Officer sends an email to PKI Sponsor's email address when responding to a request to recover any escrowed keys based on a request signed the PKI Sponsor's private key.

4.12.2.5 Notification of Key Recovery by the CA to Other Entities

There is no requirement to notify other entities of key recovery requests.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

Special care is taken to protect RA equipment, including cryptographic modules, from theft, loss, and unauthorized access at all times. RA Equipment is marked “For DoD/NSS PKI Authorized Use Only” and is physically protected as described in Section 5.1.2. Only applications required to perform PKI functions are allowed on the RA equipment.

5.1.1 Site Location and Construction

All NSS PKI RA equipment and operations are located in facilities and/or office areas approved by agency security officials as constructed for processing of classified information of the highest classification that will be asserted in or protected by use of a certificate issued by or through that equipment or SECRET, whichever is higher.

5.1.2 Physical Access

The RA Officer /LRA is present whenever the cryptographic module is installed and activated.

The RA will implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. A variety of mechanisms may be used to protect the RA equipment from tampering. Any of the following are acceptable:

- The RA equipment is in a secured facility with controlled access; only people on an access list may enter the room where the RA equipment is located. The identity of people accessing the RA equipment is recorded by someone other than those accessing the RA equipment, along with access times and dates;
- The RA equipment is located in a facility controlled at a level above the classification of the network to which it is connected and only people with appropriate clearances are allowed unescorted access to the RA/LRA equipment;
- When not in use, the RA equipment is in a locked container as specified below for storage of cryptographic modules, to which only authorized RAs have access;
- Tamper evident seals are placed on the RA equipment in access controlled facilities, and these seals are inspected weekly by the RA Officer or IAO – a record of the inspections is maintained for inspection during compliance audits.

The PKI Sponsor keeps the deactivated cryptographic module under the direct physical control or locks the token in a container to which only that person has access. In unclassified spaces (normally a government controlled space), RA tokens are stored in a safe, securely locking file cabinet or similar container. Any loss of control is immediately reported to an RA Officer.

5.1.3 Power and Air Conditioning

RA equipment is supplied with sufficient power and air conditioning sufficient to provide reliable operation.

5.1.4 Water Exposures

Except in tactical environments, RA equipment is installed in a manner to preclude water damage. In areas susceptible to flooding, moisture detectors are installed. In a tactical environment, the RA equipment will be protected from water damage to the extent operationally feasible.

5.1.5 Fire Prevention and Protection

Except in tactical environments, RA equipment is installed in a manner to minimize the potential of fire damage. Smoke detectors are installed. In a tactical environment, the RA equipment will be protected from fire damage to the extent operationally feasible.

5.1.6 Media Storage

All media is stored away from sources of heat, and away from obvious sources of water (e.g., away from water pipes) or other obvious hazards to the extent possible based on the operational situation. Electromagnetic media (e.g., tapes, diskettes) are stored away from obvious sources of strong magnetic fields (e.g., audio speakers, monitors). Material not required for daily operation or not required to remain with the RA equipment is stored in a room or building separate from the RA equipment until it is transferred to the archive location.

RA Officer/TAs control tokens that do not contain private keys such that they are not subject to unauthorized access.

The RA Officer handles, packages and stores media containing private key material as SECRET unless the cryptographic module is specifically approved as unclassified when locked. The RA Officer advises PKI Sponsors of this requirement and the requirements to protect keys as specified in Section 5.1.2. In addition to the above, RA Officer private key material is protected as specified in Section 6.2.

5.1.7 Waste Disposal

RA Operations Staff remove and destroy normal office waste as specified in local policy. Classified media and papers, and media used to collect information as specified by Section 9.4 is destroyed using processes approved for the destruction of classified information.

Media containing private key material is destroyed using an NSA approved process for the destruction of SECRET materials.

5.1.8 Off-site Backup

The IAO or SA will back up the RA electronic audit logs monthly using the audit log backup procedures. Audit log backup will be stored as specified in Section 5.4.5.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.

Since improper actions, whether malicious or inadvertent can weaken the integrity of the CAS, all persons filling trusted roles related to RA operations are held accountable to perform designated actions correctly.

The functions performed in these roles form the basis of trust in the entire NSS PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

DISA or the approving RA Officer forwards contact information, including names, organizations, and contact information, of RA Officers to the CAS when the RA is established and whenever there are changes to the list. RAs maintain a list of SAs, IAOs, and TAs supporting the RA.

The only trusted roles defined by this RPS are the RA Operations Staff (including RA Officers), TAs, and Security Auditors.

5.2.1.1 CAS Operations Staff

Not applicable.

5.2.1.2 RA Operations Staff

RA Operations Staff consists of the SA and the RA Officer, and are the individuals holding trusted roles that operate and manage RA components. RA Operations Staff is responsible for the following:

- Installation, configuration, and maintenance of the RA;
- Establishing and maintaining RA operating system and application accounts; and,
- Routine operation of the RA equipment such as system backup and recovery or changing recording media.

RA Officers are considered part of the RA Operations Staff and may perform some or all of the above functions. In addition, RA Officers are specifically responsible for the following:

- Registering new Name Subscriber and requesting the issuance of certificates (RA/LRA);
- Registering new Role and System and Device Subscriber and requesting the issuance of certificates (RA Only);
- Verifying the identity of PKI Sponsors (RA/LRA);
- Verifying the accuracy of information included in certificates (RA/LRA);
- Approving and executing the issuance of certificates (RA/LRA);
- Requesting (RA/LRA), approving, and executing the suspension, restoration, and revocation of certificates (RA only);

- Verifying the identity and authorization of entities requesting recovery of escrowed key material (RA/LRA);
- Authorizing and facilitating the recovery of escrowed key material (RA Only);
- Recovering escrowed key material if assigned that responsibility by the ANMA (RA Only);
- Generating keys for Code Signing Certificates (RA Only);
- Distributing recovered copies of escrowed keys to requestors, with protection as described in Sections 6.2.6 and 6.4.1 (RA Only); and,
- Initializing and distributing SIPRNET hardware tokens and user information on control of the token and PIN. (RA/LRA).

5.2.1.3 Trusted Agent

A Trusted Agent is defined in Section 1.3.4 as an individual holding a trusted role that assists in performing RA Officer responsibilities. However, a TA does not have privileged access to any CAS components to authorize certificate issuance, certificate revocation, suspension, restoration, or key recovery. A TA may be responsible for the following:

- Verifying the identity of PKI Sponsors;
- Verifying the accuracy of information to be included in certificates;
- Verifying the identity and authorization of entities requesting certificate revocation, suspension, or restoration;
- Verifying the identity and authorization of entities requesting recovery of escrowed key material.; and,
- Initializing (if authorized by CC/S/A) and distributing SIPRNET hardware tokens and user information on control of the token and PIN.

5.2.1.4 Security Auditor

RA Security Auditor is the RA IAO and is responsible for auditing RAs as defined in Section 5.4. Security Auditors are responsible for the following:

- Reviewing, maintaining, and archiving audit logs; and,
- Performing or overseeing internal audits to ensure that RAs are operating in accordance with the associated CPS and RPS.

5.2.2 Number of Persons Required per Task

See [CAS CPS] for CA related information.

Third Party Key Recovery is the only required multi party control activity described in this RPS and the process uses two RAs to accomplish it as described in Section 4.12.2.

5.2.3 Identification and Authentication for Each Role

All PKI related communications between a TA and an RA Officer or between RA Officers is digitally signed using the *id-CNSS-hardware* Name Signature certificate issued to the individual.

If necessary for privacy or to protect “need to know” (e.g., transfer of activation data), information will be encrypted using the *id-CNSS-software* Name encryption certificate. RA Officer communication to the CA is authenticated and encrypted using Client-authenticated TLS using the RA Officer’s *id-CNSS-hardware* Name Identity certificate and the CA Device certificate.

RA Officer credentials are only used for RA functions.

Local users authenticate to the RA workstations using a strong password or, if joined to a domain enabled for certificate based login, using their *id-CNSS-hardware* Name Identity certificate.

The RA Officers for a CC/S/A operating under this RPS are nominated by the CC/S/A to the ANMA for appointment/approval. Other trusted roles within the CC/S/A are nominated by the local command. An RA Officer appoints/approves LRAs and TAs that will work with the RA Officer to provide PKI services and SA and IAO personnel for the RA Workstation. An LRA appoints/approves TAs that will work with the LRA and SA and IAO personnel for the LRA Workstation.

Appointment/approval is documented in a formal appointment memorandum. Individuals acknowledge the appointment to a trusted role using the [DD FORM 2841] or by endorsement of the appointment memo to the appointing official. Acceptance may be via wet signature or digital signature using the individual’s *id-CNSS-hardware* Name Signature certificate. A copy of the appointment and acknowledgement are sent to the primary CC/S/A RA Officer for inclusion in the archives.

5.2.4 Roles Requiring Separation of Duties

The Security Auditor (IAO) for an RA has no other trusted role within the NSS PKI.

No RA Officer holds any other trusted role on the CAS.

Compliance auditors appointed by the DoD PKI PMO never perform any other role on the RA undergoing Compliance Audit.

Only the IAO performs security audit function on the RA equipment.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

The nominating official is responsible for ensuring that all personnel nominated to fill a trusted role comply with the following:

- Be employees of a CNSS member agency or be a contractor/vendor employee contracted to a CNSS member agency;
- Be within the administrative control of an identified administrator who is a CNSS member agency employee or a civilian contractor/vendor employee of equivalent or greater responsibility and compensation;
- Have not been denied a security clearance or had a security clearance revoked;
- Be appointed in writing;

- Hold a minimum clearance of a final U.S. SECRET;
- Be a U.S. citizen;
- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 5.2.1;
- Have not been previously relieved of trusted role duties for reasons of negligence or non-performance of duties; and,
- Have not been convicted of a felony offense.

The nomination is signed by the nominating official via wet signature or digital signature using the individual's id-CNSS-*hardware* Name Signature certificate.

5.3.2 Background Check Procedures

The nominating official is responsible for ensuring that all personnel nominated have a final U.S. SECRET Clearance (as stated in Section 5.3.1). The release of details with respect to the individual's background check information is under the control of the individual's local security office.

5.3.3 Training Requirements

All personnel assigned to a trusted role under an RA (RA Officer, IAO, SA, TA) are provided with training on the stipulations of [CNSSI 1300], any appropriate local guidance, and the PKI duties they are expected to perform (e.g., LRA, Registration/Revocation, Key Recovery). RA Operations Staff are also instructed on RA operational and security principles, mechanism, and procedures to include disaster recovery and business continuity, and any PKI specific details of the software/hardware that is used for RA operations. RA Officers trained for the DoD PKI SIPRNET Pilot do not require initial training.

All individual training is documented in the individual's local training record.

5.3.4 Retraining Frequency and Requirements

Significant changes to RA operations are generally covered in CAS level training awareness plans. The office that nominates CC/S/A RA Officer's determines if there is a need for other training. All individual training is documented in training records maintained by the organization.

5.3.5 Job Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

The CC/S/A official with administrative/disciplinary authority over the individual is notified of violations of [CNSSI 1300], the applicable CPS/RPS or other procedures along with an ANMA recommendation for action. The CC/S/A official determines the appropriate action.

Any person, including the ANMA, who becomes aware of a suspected security violation or compromise, reports the suspected security violation or compromise to the appropriate security officials.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to operate any part of the PKI are subject to the same criteria as a US Government employee and are cleared to the level of the information protected by the certificates the PKI issues. The contracts of these contractor personnel will stipulate that the contractor will be liable for any loss associated with any violation of the CP or this RPS, to include misuse of the equipment provided to it (e.g., private key, certificate, hardware token, and work station).

If a vendor provides RA services to the DoD via a subcontractor, the vendor will establish written procedures to ensure that any subcontractors perform in accordance with this RPS. Such procedures are made available during compliance audits.

5.3.8 Documentation Supplied to Personnel

The CC/S/A Primary RA Officer determines the documentation (if any) required for each role. If there is documentation, it is provided during training. If the documentation is updated each appropriate individual receives a copy of the update.

RA Officers, SAs and IAOs are provided appropriate system, application and cryptographic module documents that are retained at the RA location. They will have access to:

- Operating System and application on-line documentation (help files); and,
- ANMA approved RPS.

TAs will have:

- ANMA approved RPS; and,
- Local operating procedures, if provided by CC/S/A RA Officer /LRA.

The CC/S/A RA Officer determines if other documentation is required for each role. If the documentation is updated each appropriate individual receives a copy of the update.

5.4 AUDIT LOGGING REQUIREMENTS

Audit log files are generated for all events related to the security of the CAS or RA. Where possible, security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical or electronic mechanism is used. Physical logbooks are bound to allow for the detection of the removal of pages. Logbooks are bound and entries are made in indelible ink providing protection against removal of pages and against alteration or deletion of entries. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits. The security audit log for each auditable event defined in this section is maintained in accordance with Section 5.5.2.

5.4.1 Types of Events Recorded

Any security auditing capabilities of the underlying RA equipment operating system are enabled during installation.
No matter what form, audit entries captured in RA operation include:

- The type of event;
- The date and time the event occurred;
- For signing, revocation, escrow, or recovery processes, a success or failure indicator;
- The identity of the entity or operator that caused the event; and,
- For messages from any source requesting an action by the RA, the message date and time, source, destination and contents.

At a minimum, the events identified in the Table 5-1 are recorded by each system that performs the action:

Table 5-1: Auditable Events

Event Type	Event	Where recorded
Security Audit	• Any changes to the Audit parameters, e.g., audit frequency, type of event audited • Any attempt to delete or modify the Audit logs	• IAO Manual log/ Operating System Log • Operating System Log
Identification and Authentication	• Successful and unsuccessful attempts to assume a role	• Operating System Log
	• The value of maximum authentication attempts is changed	• Operating System Log
	• The maximum number of unsuccessful authentication attempts occurs during a user login • Operating System Log	• Operating System Log
	• An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	• Operating System Log
	• An Administrator changes the type of authenticator, e.g., from password to biometrics	• Operating System Log
Local Data Entry	• Any security-relevant data that is entered in the system (e.g., account management, directory access, policy or privilege change)	• Operating System Log
Remote Data Entry	• Any security-relevant messages that are received by the system	• Operating System Log/email Logs

Event Type	Event	Where recorded
Data Export and Output	• Any successful and unsuccessful requests for private, sensitive, classified, or security-relevant information	• Operating System Log
Key Generation	• Whenever the CAS generates a key (Not mandatory for single session or one-time use symmetric keys)	• Not applicable
Private Key Load and Storage	• The loading of Component private keys • Any access to certificate subject private keys retained within the CAS for key recovery purposes	• Operating System Log
Trusted Public Key Entry, Deletion, and Storage	• Any changes to the trusted public keys, including additions and deletions	• Operating System Log
Private Key Export	• The export of private keys (keys used for a single session or message are excluded)	• Operating System Log
Certificate Registration	• Any certificate requests	• Email/manual Logs
Certificate Status	• Any certificate revocation, modification, suspension, re-key, or renewal requests	• Email/manual Log
Certificate Status Change Approval	• The approval or rejection of a certificate status change request	• Email/manual Log
CAS or RA Configuration	• Any security-relevant changes to the configuration of the CAS or RA • Configuration changes to the CAS or RA involving hardware, software, operating system, patches, or security profiles.	• See Configuration Documentation
Account Administration	• Roles and users are added or deleted	• Operating System Log
	• The access control privileges of a user account or a role are modified	• Operating System Log
Certificate Profile Management	• All changes to the certificate profile	• Not applicable
Revocation Profile Management	• All changes to the revocation profile	• Not applicable
CRL Profile Management	• All changes to the CRL profile	• Not applicable
Personnel Controls	• Appointment of an individual to a trusted role	• Email/manual Logs
	• Designation of personnel for multiparty control	• Not applicable
	• Training of individuals appointed to the RA role	• Organization Training records
Miscellaneous	• Installation of CAS and RA operating systems and applications	• Operating System Logs
	• Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring, or destruction of cryptographic	• Manual Log

Event Type	Event	Where recorded
	modules	
	• Installing hardware cryptographic modules	• Operating System Log
	• Removing hardware cryptographic modules	• Operating System Log
	• Receipt, servicing (e.g., keying or other cryptologic manipulations), and shipping hardware cryptographic modules	• Manual Log
	• System startup	• Operating System Log
	• Logon attempts to CAS or RA applications	• Not applicable
	• Receipt of hardware / software	• Manual Log
	• Attempts to set passwords	• Operating System Log
	• Attempts to modify passwords	• Operating System Log
	• Backing up CAS or RA internal databases	• Manual Logs
	• Restoring CAS or RA internal databases	• Manual Logs
	• File manipulation (e.g., creation, renaming, moving)	• Operating System Log
	• Posting of any material to a repository	• Not applicable
	• Access to CAS or RA internal databases	• Operating System Logs
	• All certificate compromise notification requests	• Email/manual Logs
	• Re-key of the any component private keys to include the CAS	• Not applicable
	• A message from any source received by any CAS requesting an action related to the operational state of the CAS	• Not applicable
	• Any requests and actions taken in response to messages requesting CAS actions not covered elsewhere	• Not applicable
	• Installation, access, and modification (to include changes in configuration files, security profiles, and administrator privileges) of CAS and RA system	• Operating System Logs
	• Any use of the CA signing key	• Not applicable
	• Any use of the RA signature key	• Not applicable
	• Messages received from any source requesting RA actions, (certificate requests, compromise notification, key recovery requests, key recovery approval)	• Email/manual Logs
	• Any actions taken in response to requests for RA actions	• Email/manual Log
Physical Access	• Personnel access to room housing CAS	• Not applicable

Event Type	Event	Where recorded
and Site Security	• Physical access to the CAS	• Not applicable
	• Known or suspected violations of physical security	• Manual Log
	• Any known or suspected violations of physical security, suspected or known attempts to attack the RA equipment via network attacks, equipment failures, power outages, network failures, or violations of this certificate policy	• Manual Log
Anomalies	• Software error conditions	• Operating System Log
	• Software check integrity failures	• Operating System Log
	• Receipt of improper messages	• Email/manual Log
	• Misrouted messages	• Email/manual Log
	• Network attacks (suspected or confirmed)	• Manual Log
	• Equipment failure	• Manual Log
	• Electrical power outages	• Manual Log
	• Uninterruptible power supply (UPS) failure	• Manual Log
	• Obvious and significant network service or access failures	• Manual Log
	• Violations of certificate policy	• Manual Log
	• Violations of certification practice statement	• Manual Log
	• Resetting operating system clock	• Operating System Log
	• Network failures	• Manual Log
Key Escrow and Recovery	• Server installation, access, and modification (to include changes in configuration files, security profiles, administrator privileges)	• Not applicable
	• Key escrow database application access (e.g., logon/logoff)	• Not applicable
	• Messages received from any source requesting key escrow database actions, (e.g., escrowed key retrieval requests)	• Manual Logs
	• Messages sent to any destination authorizing key recovery actions, (e.g., first party escrowed key retrieval authorizations, second party key recovery approvals)	• Manual Logs
	• Actions taken in response to requests for key escrow database actions	• Manual Logs
	• Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying key escrow database cryptographic modules	• Not applicable

Event Type	Event	Where recorded
	- Receipt of keys for escrow and posting of these keys to the key escrow database	- Not applicable
	- Retrieval, packaging (e.g., keying or other cryptologic manipulations), securing, and shipping copies of escrowed keys;	- Manual Log
	- Transfer of escrowed keys to requestors	- Manual Log
	- Any security-relevant actions performed in support of delivery of escrowed keys	- Manual Log
	- Requestor identity and authorization verification (including copies of authorizations; e.g., court orders) supporting key recovery requests	- Manual Log

5.4.2 Frequency of Processing Log

The IAO reviews the RA manual and operating system audit logs monthly. The review includes at least 33% of the data collected since the last audit.

5.4.3 Retention Period of Audit Log

The information generated on the RA equipment is kept on the RA equipment until the information is moved to an appropriate archive facility. The IAO conducts a review prior to deletion from the operational system. Only the IAO ever deletes security audit data from the RA equipment. Security audit data is retained on-site for at least two months, then off-site as archive records in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

The operating system interface allows only persons with administrator privileges (i.e., IAO and SA) to start, stop, view, backup, modify, delete, or otherwise manage audit logs. The IAO investigates any suspicious gaps in the audit record that might indicate unauthorized deletion of audit records.

Until transferred to the offsite archive facility, audit data is retained either on the RA equipment or secured in a facility under the direct control of the IAO.

The SA or IAO checks on a weekly basis to ensure there is sufficient space for at least two weeks of audit data. If there is not sufficient space, the IAO copies off the current audit data and deletes sufficient records to ensure sufficient space.

The RA Officer transfers all filled log books to the IAO. The SA transfers all backups of operating system logs and electronic records to the IAO. The IAO ensures that the RA Officer has no access to audit records in his/her control. The IAO or SA deletes on-line audit data only after successfully creating the backup and transferring control of the archived audit files to the IAO.

5.4.5 Audit Log Backup Procedures

The IAO or SA will back up the RA operating system audit log monthly using the audit log backup procedures. Each month, a copy of that month's backup(s) will be moved to an offsite facility.

5.4.6 Audit Collection System (Internal Vs. External)

The audit system is internal to the RA equipment and is configured to be invoked on system startup and cease operation only at system shutdown. There is no "RA Application" or separate application logs. The RA Officer does not have the privileges to impact, in any way, audit configuration.

If the audit function overflows or otherwise ceases to function, the RA Officer will not perform RA functions, except entering revocation/suspension information on the CA, until the audit data can again be collected. Immediately after backing up audit data from the workstation and restarting the auditing function, the IAO will open a ticket with the DISA Helpdesk (disa-esmost@okc.disa.mil) identifying the RA Officers by their certificate CNs and the fact that the Audit Data Overflowed along with the period for which CA audit data must be reviewed (beginning of audit failure event to time when audit function is restored). The Ticket will request that the CA administrator review the CA server audit data to ensure that the RA Officers have not performed any functions other than revocation/suspension during the time period specified.

5.4.7 Notification to Event-Causing Subject

No notification is given to event-causing subjects.

5.4.8 Audit Log Assessments

The IAO will, as part of its security audit review, verify that the audit logs have not been tampered with by checking audit configuration and the continuity of security audit data. Then review the data for events such as account creation, changes to accounts, changes to audit parameters, changes to password, failed login attempts, access violations, repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Suspicious activity will be logged/explained in an audit log summary and reported to the local site administrator or commander (not to the RA Officer). If a subsequent investigation finds fraudulent behavior, then the IAO reports this result to the ANMA through the CC/S/A CPMWG Representative. The IAO records the results of the audit log review by making an audit log summary entry in the log book.

The RA Officer and RA SA and IAO will be watchful for anomalies and attempts to violate the integrity of the system, including the equipment, its physical location, and its personnel.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

When determining if a specific item should be placed in the archive, the RA uses the following as a guide: "Archive records shall be sufficiently detailed to establish the validity of a signature and determine the proper operation of the RA." At a minimum, that RA archives the following data – using the described mechanisms:

- RA system equipment configuration and updates – physical record;
- RA System Certification and Accreditation documentation – paper or electronic records;
- All RPSs that the RA has been operating in accordance with – paper or electronic record;
- Any contractual or other agreements related to RA operations – paper or electronic record;
- All security audit data as defined in Section 5.4.1 – in electronic or paper form as appropriate;
- Appointment of individual to a trusted role – Physical record;
- Audit review summaries, actions taken as a result of the review, and other remedial actions such as resulting from anomalies detected by the DoD NSS Subordinate CAS operations staff – Physical record;
- Subscriber and RA identity authentication documentation as required by Section 3.2.3.1 – physical record [DD FORM 2841] and [DD FORM 2842];
- Documentation of receipt and acceptance of certificates/subscriber agreements as described in Section 4.4.1 – physical record [DD FORM 2841] and [DD FORM 2842] or electronic record digitally signed with a hardware certificate;
- Documentation of receipt of tokens - paper record or electronic record digitally signed with a hardware certificate;
- All requests to create certificates (including any hard copies) – in electronic or paper form as appropriate;
- All requests to revoke/suspend/restore certificates (including any hard copies) – in electronic or paper form as appropriate;
- Documentation of the identity of the recipient of an escrowed key – in electronic or paper form as appropriate;
- Documentation of the reason for key recovery – in electronic or paper form as appropriate;
- Documentation of the verification of authorization for recovery of escrowed key – in electronic or paper form as appropriate;
- Software applications and associated software user documentation required to access electronic archive records – appropriate electronic media;
- All work related communications to or from the PMA, the ANMA, other CMAs, and compliance auditors, including remedial action reports – in electronic or paper form as appropriate;
- Violations of the CP or applicable CPS/RPS - in electronic or paper form as appropriate; and,

- Compliance Audit Reports – paper.

The current physical audit log (e.g., log book) and other paper audit records will be stored in a locked container to which only RA personnel have access. Only RA personnel will have access to the physical log and only authorized RA Officers will make entries in it. Paper log books are bound, so as to make removal of pages evident, and all entries are made using non-erasable ink.

Note: The RA maintains the current [CNSSI 1300] and [CAS CPS] but does not maintain them as part of the RA archive as they are archived at a higher level.

5.5.2 Retention Period of Archive

RA Archive records are kept for a period of ten years and six months. Electronic data is placed on CD-ROM/DVD when removed from the originating workstation.

5.5.3 Protection of Archive

The IAO will maintain a list of authorized persons with access, modify, and/or delete to archive data and provides it to the RA Officer.

CD-ROM/DVD is used for long term storage of electronic media and does not degrade within the required archive period. Only IAO personnel will have access to original archive data. The SA transfers all backups of operating system logs and electronic records to the IAO. Estimated data retention of the media exceeds the required archive period.

Paper records required to be archived in accordance with Section 5.5.1 are transferred by the RA Officer to the IAO when they are no longer required for ongoing RA operations.

The IAO ensures that the RA Officer has no access to audit records in his/her control.

The IAO controls release of the archive data and ensures that sensitive archive information is only be released in accordance with Section 9.4.

Archive data is kept in a location separate from the RA site in a safe, secure storage facility. The archive data is labeled with the RA workstation designation, the date, and classification prior to being placed in the archive.

All archive data is stored and protected as SECRET.

5.5.4 Archive Backup Procedures

Archive information is not backed up.

5.5.5 Requirements for Time-Stamping of Records

The RA electronic records use the system clock on the RA Workstation. The RA personnel use the workstation clock for the time on manual records.

5.5.6 Archive Collection System (Internal vs. External)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain and Verify Archive Information

Not applicable.

5.6 KEY CHANGEOVER

Not applicable.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

If a hacking attempt or other form of potential compromise of a RA workstation or RA credential becomes known, the IAO initiates an investigation in order to determine the nature and the degree of damage.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

If it becomes necessary to rebuild the RA workstation, the RA Officer will ensure that the SA first captures existing system audit data to the extent possible. If audit data cannot be completely captured, the IAO will ensure that the RA documents the extent of audit data lost in the RA manual log.

5.7.3 Entity Private Key Compromise Procedures

In the event of the compromise of an RA Officer's private key, the revoking RA Officer investigates to determine the earliest known good time of the RA certificate and enters the revocation information on the CA for the certificate corresponding to the compromised key using the date determined as the date of compromise. The revoking RA Officer forwards a request to the CAS to identify certificates issued based on the compromised key from the date of compromise and to identify any private keys recovered based on authentication from the compromised key. The revoking RA Officer revokes any certificates identified. Affected Subscribers are notified and directed to apply for new certificates if still required.

In the event of the compromise of a TA key, the revoking RA Officer investigates to determine the earliest known good time of the TA certificate and enters the revocation information on the CA for the certificate corresponding to the compromised key using the date determined as the date of compromise. The revoking RA Officer reviews the records of subscriber certificates issued and keys recovered to identify actions based on the compromised TA key from the date of compromise. The revoking RA Officer revokes any certificates identified. Affected Subscribers are notified and directed to apply for new certificates if still required.

5.7.4 Business Continuity Capabilities after a Disaster

Not applicable.

5.8 CA, RA, OR TA TERMINATION

5.8.1 CA Termination

Not applicable.

5.8.2 RA Termination

If an RA is terminated, the RA Officer's RA certificates are revoked. If the termination is for cause (e.g., negligence, possible unauthorized use of the private key), all certificates issued or recovered based on that RA certificate are revoked. See Section 5.7.3. Affected Subscribers are notified and directed to apply for new certificates if still required. The revoking RA Officer notifies the CAA to remove the terminated RA Officer from the RA Officer from any privilege group on the CA.

For any RA termination, another RA takes possession of any archive records and any security audit logs since the last archive maintained by that RA. If there is no available RA, the CC/S/A transfers the RA archive records a designated the CC/S/A archive facility.

5.8.3 TA Termination

If a TA is terminated for cause (e.g., negligence, possible unauthorized use of the private key), it is treated as a compromise effective the date when the activity causing the termination started. See Section 5.7.3. TAs do not maintain archive records.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

A private key is considered to be generated by the NSS PKI entity that first comes into possession of it: Subscriber, PKI Sponsor, RA Officer, or CAS.

All Name and Role subscriber key generation and Pseudo-random numbers used for key generation are generated using a FIPS approved method on the NSA approved token or hardware cryptographic module. System and Device subscriber certificate key generation and Pseudo-random numbers used for key generation are generated using a FIPS approved method on the NSA approved software or hardware cryptographic module.

Subscriber private keys associated with certificates that assert the *id-CNSS-hardware* Policy OID, to include RA keys, are generated on the Subscriber token – an NSA approved device. Encryption keys are generated off token as described in [CAS CPS], placed in escrow, and inserted into the Subscriber token during the issuance process. The NSA token selection criterion precludes tokens which can export the private key.

The private key associated with the *id-CNSS-device* Policy OID that is generated in software modules is only exported in encrypted form.

6.1.2 Private Key Delivery to Subscriber

In all cases, PINs, Passwords, PKCS#12 files (p12 files), and tokens not approved by NSA as unclassified[3] used on the SIPRNET are treated as classified SECRET. Physical transfer is always done in a manner approved for the transfer of classified information.

For keys and certificates being delivered on an NSA approved hardware token (e.g., smartcard, USB), the keys are protected by a PIN as specified in Section 6.4.1. After the keys and certificates are generated by the RA Officer or recovered to a token, the RA Officer immediately places the keyed token into a serialized tamper-evident envelope. If not shipped immediately, the envelope will be stored in a locked container and the PIN is secured in a separate container, approved for classified storage until shipment. The keyed token and PIN are delivered to the PKI Sponsor (Requestor is the PKI Sponsor for a key recovered to a token) in one of the following ways:

(PKI Sponsor and TA) The token, in the tamper evident package, is prepared for shipment as classified information unless it is specifically approved as unclassified. It is sent to the PKI Sponsor using continuously accountable means (e.g., US Registered Mail with return receipt, Federal Express). If the RA Officer has been provided with a PKI Sponsor email address, the RA Officer sends a digitally signed email to the PKI Sponsor with the serial number for the seal and expected delivery date. The RA Officer sends the PIN to the TA via signed and encrypted email on SIPRNET using NSS PKI. The TA authenticates the PKI Sponsor's identity and

[3] The SC 650 token has been approved by NSA as unclassified when locked.

obtains a signed Certificate of Acceptance and Acknowledgement of Responsibilities before delivering the PIN to the PKI Sponsor.

(Two TAs) The token, in the tamper evident package, is prepared for shipment as classified information unless it is specifically approved as unclassified. It is sent to the TA assisting the RA Officer using continuously accountable means (e.g., US Registered Mail with return receipt, Federal Express). The RA Officer sends a digitally signed email with the serial number for the seal and expected delivery date to the TA. The RA Officer sends a second TA the PIN via digitally signed and encrypted email on SIPRNET using NSS PKI at the same time the token is shipped. The two TAs are present and present the PIN and token to the PKI Sponsor after one of the TAs authenticates the PKI Sponsor's identity and obtains a signed Certificate of Acceptance and Acknowledgement of Responsibilities.

(PKI Sponsor with CNSS PKI) The token, in the tamper evident package, is prepared for shipment as classified information unless it is specifically approved as unclassified. It is sent to the PKI Sponsor using continuously accountable means (e.g., US Registered Mail with return receipt, Federal Express). If the RA Officer has been provided with a PKI Sponsor email address, the RA Officer sends a digitally signed email to the PKI Sponsor with the serial number for the seal and expected delivery date. Upon receipt of the Subscriber acknowledgment of receipt of the token (digitally signed email or a signed Certificate of Acceptance and Acknowledgement of Responsibilities), the RA Officer sends the PIN to the PKI Sponsor via a digitally signed and encrypted email on SIPRNET using NSS PKI. Alternatively, the RA Officer may ship it to the PKI Sponsor via continuously accountable means. In this case, and if the RA Officer has been provided with a PKI Sponsor email address, the RA Officer sends a digitally signed email to the PKI Sponsor with the shipping date, method of shipping, and expected delivery date.

An RA Officer that uses the 90Meter Certificate Issuance Workstation - Batch software for bulk enrollment may send the PINs for individual tokens as specified above or the RA Officer may send the log file with multiple PINs. If sending multiple PINs, the RA Officer only sends the PINs to a TA and ensures that only the PINs for the PKI Sponsors at the TA's location are sent to the TA.

If the PKI Sponsor or TA suspects that the delivery of either the token or PIN may have been compromised, the RA Officer will revoke the certificates. If, upon receipt of the PIN, the PKI Sponsor is not able to activate the Token, the PKI Sponsor reports this to the RA Officer or TA. This is treated as a compromise of the private key and the certificates are revoked and, if needed, a new set of certificates issued.

The PKI Sponsor is told to change their PIN when they receive a keyed PKI Token. If a new CRI is required by the implementation to perform PIN Reset, the RA Officer generates and sends a new CRI form to the PKI Sponsor with the PIN.

The RA Officer will require the PKI Sponsor to return a delivery receipt for the activation data.

Keys and certificates that are stored in a P12 file are protected by a password of 20 or more characters with a minimum of two upper, two lower, two numbers and two special characters interspersed throughout the password. P12 files are never retained on the computer in an unencrypted form. RA Officers immediately delete P12 files once they have been processed for transfer. Personnel receiving P12 files are advised to immediately remove the file from the file system once the keys have been imported into the user’s cryptographic module.

For software key recovery, the 2nd RA Officer receives recovered encryption keys in a P12 (PKCS12) file as described in Section 4.12.2.3. The 1st RA Officer receives a system generated password for the P12 file. The password does not resemble dictionary words; differs from words or names by at least two characters that are not simple number-for-letter substitutions and does not consist of words or names followed by 1-4 digits. The password/passphrase also does not contain sequences, repeated characters, date formats, or license plate formats.

When possible, the P12 file will be delivered directly to the requestor in an encrypted email using the requestor’s *id-CNSS-software* Name encryption certificate. If the requestor does not have a valid NSS Email Encryption certificate, the .p12 file will be written to removable media (e.g., CD-ROM, DVD), immediately placed into a serialized tamper-evident envelope, and delivered to the requestor directly using continuously accountable means (e.g., US Registered Mail with return receipt, Federal Express). If not shipped immediately, the envelope will be stored in a locked container until shipment.

In either case, the requestor is directed to acknowledge receipt of the P12 file to the 2nd RA Officer (digitally signed email or a signed Certificate of Acceptance and Acknowledgement of Responsibilities).

Once the 2nd RA Officer has received the acknowledgement, the 1st RA Officer then sends the password to the requestor via a digitally signed and encrypted email using *id-CNSS-software* Name encryption certificate. If the requestor does not have a valid *id-CNSS-software* Name encryption certificate, the 1st RA Officer ships it to the requestor via continuously accountable means.

If the requestor suspects that the delivery of either the P12 file or password may have been compromised, they immediately notify the sending RA Officer, and the RA Officer will revoke the certificate and notify the PKI Sponsor if not part of the process. Once the process is completed, the RA Officer destroys all copies of the P12 file.

6.1.3 Public Key Delivery to Certificate Issuer

Not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

The primary method for DoD relying parties to obtain the NSS Root, Intermediate and Signing CA signing certificates is via controlled service/agency standard software load (e.g., gold disk). The CC/S/A RA Officer interacts with the service/agency organization responsible for maintaining the standard software load to advise them of changes that are required.

The RA Officer provides the NSS Root CA, Intermediate CA, and Signing CA signing certificates to any relying party that requests it by directing them to http://iase.disa.smil.mil/pki-pke. The CRI issued to the Subscriber has a hash of the Root certificate which is used to verify the self-signed certificate.

6.1.5 Key Sizes

Not applicable.

6.1.6 Public Key Parameters Generation and Quality Checking

For Subscriber encryption keys, see [CAS CPS]. Other Subscriber RSA key pairs are generated and checked on the NSA approved cryptographic module in compliance with FIPS 186-3.

Requirements related to selection of domain parameters is not applicable, as the PKI is using the RSA algorithm.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Not applicable.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The Subscriber hardware token is the SAFENET 650. Other hardware tokens or software cryptographic modules are selected from a list maintained by the DoD PKI PMO. The PMO process for maintaining the list ensures that the token and associated middleware or software cryptographic module is approved by NSA for use in the DoD implementation of the NSS PKI.

For hardware tokens, the CC/S/A RA Officer who initially acquires the tokens is responsible for ensuring that the tokens are accounted for. That RA Officer may distribute tokens singly or in bulk. Tokens may be distributed to individual PKI Sponsors, RA Officers or TAs. Unless the token is hand delivered, the tokens are sent in serialized tamper-evident packaging using continuously accountable means (e.g., US Registered Mail with return receipt, Federal Express). The person sending the tokens sends a digitally signed email to the recipient stating the serial number of the seal and the expected arrival date. Upon receipt, the recipient verifies that there is no evidence of tampering and then acknowledges receipt in a digitally signed email. The sending RA Officer maintains a log of all tokens issued and the identity of the RA Officer/TA that received the token in the RA audit records.

Recipient RA Officers may further distribute tokens to RAs or TAs operating under them using the process described above.

If there is evidence of tampering, the recipient advises the transmitting RA Officer. If the recipient is a TA, the TA returns the entire shipment to the RA Officer. The first RA Officer to receive the returned tokens destroys them. If the first RA Officer is not the originating RA Officer, the originating RA is advised date of destruction and the serial numbers of the tokens involved.

If not done prior to receipt, the tokens used by Name or Role subscribers that require initialization are initialized by an RA prior to issuance to the PKI Sponsor.

See Section 4.12.2 for RA processes to ensure security of escrowed keys.

Name certificates that assert non-Repudiation are under the exclusive control of the PKI sponsor when they are generated or, if generated by the RA, once the Sponsor acknowledges receipt of the key.   Role and System or Device certificates never assert non-Repudiation.

The SAFENET 650 is approved by NSA in CNSS 014-2010, *Approval of Continued Use of SC650 Token – DECISION MEMORANDUM* [CNSS 014-2010] as a Subscriber hardware token and is unclassified when removed from the workstation. [CNSS 014-2010] provides detailed instructions for control of the SAFENET 650 token. If NSA approves other token for use, the approval may provide additional instructions related to use of the token. The RA Officer or TA informs the PKI Sponsors of the instructions provided in the NSA approval memo.

6.2.2 Private Key (n out of m) Multi-Person Control

Not applicable.

6.2.3 Private Key Escrow

Not applicable.

6.2.4 Private Key Backup

For Name or Role *id-CNSS-hardware* certificates, PKI Sponsors are not permitted to backup or otherwise copy their own private keys.

If the token can export keys, the PKI Sponsors are told to never backup or copy Subscriber private keys from the token.

If the PKI Sponsor receives a copy of the encryption private key via the key recovery process, the sponsor is reminded of the requirement to store the .p12 file only on removable media, not to back it up on-line, and to protect continuously the private key at least at a level commensurate with the level of the data the key provides access to or protects as outlined in Section 6.2.7.

For Software System or Device certificates, the PKI Sponsor is permitted to make operational copies of private keys for each application that requires the key in a different location or format; however, private keys stored in each of these applications or locations are kept in cryptographic modules that have been approved by NSA. All key transfers are done from an approved cryptographic module, and the key is encrypted during the transfer. The PKI Sponsor is responsible for ensuring that all copies of private keys, including those that might be embedded in System or Device backups, are protected, including protecting any workstation on which any of its private keys reside.

6.2.5 Private Key Archival

Not applicable.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All private keys are generated in the subscriber cryptographic module or by the CA and inserted into the subscriber cryptographic module. Private keys never exist outside an approved cryptographic module except in encrypted form. For keys that will be transported outside a cryptographic module, the encryption strength must be commensurate with the strength of the key being protected. See Section 6.1.2 for details transport of private key outside the cryptographic module. Only authorized parties are given access to the password.

6.2.7 Private Key Storage on Cryptographic Module

See Section 6.2.1.

6.2.8 Method of Activating Private Key

Private keys are activated using a PIN as specified in Section 6.4.1. The user interface does not display the PIN as it is typed.

6.2.9 Method of Deactivating Private Key

PKI Sponsors are instructed to provide appropriate protection to an activated Cryptographic module to ensure there is no unauthorized access. Generally, this is being present when the module is in use. When not in use, the Cryptographic Module on a token is deactivated by removing it from the card reader or passive timeout. PIN, PKCS#12 files, and tokens used on the SIPRNet are treated as classified and are shipped using means appropriate for classified information. The PKI Sponsor removes the hardware cryptographic module and stores it in accordance with Section 5.1.2 when not in use.

Recovered encryption keys in software are deactivated by timeout feature of the software or by logging out of the workstation.

Keys for software System or Device certificates are deactivated when the system or device is shut down.

If the token has been approved by NSA as UNCLASSIFIED when locked, it may be handled as described in the approval.

6.2.10 Method of Destroying Private Key

Private keys associated with Identity or Signature certificates that do not assert *keyEncipherment* or *keyAgreement* and any keys used to transport them, where possible, are destroyed when the certificates to which they correspond expire or are revoked. Private keys associated with encryption certificates are destroyed when they are no longer needed. The approved method(s) used for the destruction of keys is specified in the NSA approval to use the Cryptographic Module.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

For Code Signing Certificates – the key and certificate lifetimes are 8 years. However, the RA Officer ensures that the PKI Sponsor of the Code Signing certificate is aware that the limit on active use of the private key for signing is three years, after which the private key is destroyed and, if necessary, the PKI Sponsor obtains a new certificate and key pair via the initial issuance or rekey process.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

All Name and Role Subscribers use a PIN. PINs will be a minimum of 8-16 digits in length. The individual that authenticates to the TPS to request certificates selects the PIN as part of the process. If the token allows characters other than digits, Subscribers are encouraged to use them. The SC650 is currently set during formatting to lock after 5 incorrect tries at entering the PIN. NSA should provide specific guidance when approving other tokens for use.

If the System and Device software uses activation data, it is protected by an alphanumeric pass-phrase.

People are instructed to select a PIN or pass-phrase that is not related to their personal identity, history, or environment and is also told that sequences, repeated characters or numbers, social security numbers, dictionary words or names, date or license plate formats, or other easily guessed numbers. When alphanumeric pass-phrases are used, an interspersed mix of eight characters, including at least two interspersed digits, is used. They also differ from words or names by at least two characters that are not simple number-for-letter substitutions and do not consist of words or names followed by one to four digits.

The NSA token approval may provide additional instructions on activation data. If it does, the RA Officer or TA informs the PKI Sponsors of the instructions.

If a new CRI is required by the implementation to perform PIN Reset, the RA Officer generates the CRI and provides it to the PKI Sponsor. When generating the CRI, the RA Officer verifies that the information displayed for the certificates on the token is for the PKI Sponsor making the request. If the token is not locked, PKI Sponsor may request new CRI via a digitally signed email using the *id-CNSS-hardware* Name Signature certificate on the token. Otherwise, the PKI Sponsor may request the new CRI using any available means. Prior to handing the CRI to the PKI Sponsor, the RA Officer or TA on behalf of the RA Officer verifies the identity of the PKI Sponsor as the authorized holder of the token by use of personal knowledge or the use of a government issued photo identity credential.

If the RA Officer uses the 90Meter Certificate Issuance Workstation - Batch software for bulk enrollment, the RA Officer only choses either the “random PIN” or the “Locked Token” options.

6.4.2 Activation Data Protection

Activation data should be memorized, not written down. If activation data are written down, it is classified SECRET, and will not be stored with the cryptographic module.

The PKI Sponsor is the only person authorized to have the activation data for a token containing a Name certificate once the token and activation data is in the possession of the PKI Sponsor.

RA Officers will immediately encrypt any file containing PINs and delete unencrypted versions of these files resident on any workstation.

The RA Officer provides the password for the .p12 file directly to the requestor as specified in Section 6.1.2.

6.4.3 Other Aspects of Activation Data

For transmission of activation data, see Section 6.1.2.

RA Officers change the activation data on the RA cryptographic module whenever their certificates are re-keyed.

See [CAS CPS] for CA related information.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

See [CAS CPS] for CA and Repository related information.

90Meter Certificate Issuance Workstation - Batch enrollment processing is only performed on a workstation which is configured to meet RA workstation standards and is operated and controlled as an RA workstation.

The RA workstation uses an operating system approved by the CC/S/A DAA. The workstation operating system and security products and services, including any used for remote management below, are configured in accordance with the Federal Desktop Common Configuration as modified by the CC/S/A and all applicable NSA-endorsed configuration guides (http://www.nsa.gov/ia/guidance). The RA workstation operates with the minimal number of accounts required for administration and operation.

RA workstation are either managed locally (i.e., remote login is disabled) or remote management is conducted through a Virtual Private Network. VPN Cryptography uses a minimum of 112 bit cryptography using FIPS approved algorithms.

RA workstations that are joined to the network domain will operate within the following parameters.

- If the issued RA credential has the RA, LRA or NVO PCC code in the UPN, the RA uses that UPN and associated network account to authenticate to the RA workstation to perform RA functions. If the RA credential does not have the RA or LRA PCC code, the RA Officer uses the RA Officer’s individual account. The network account used will not have privileges to perform SA or IAO functions on the RA workstation. A separate network account will be created if the individual’s normal network account provides him/her with privileges to perform SA and/or IAO functions.

- For individuals performing SA and IAO roles directly on the workstation, the individual’s network account will be the account used to authenticate to the RA workstation to perform SA or IAO functions. The workstation will be configured with the appropriate privileges for these accounts to perform the SA and/or IAO function by adding them to the Local Administration group.
- If feasible, authentication to the RA workstation will be via Certificate Based Logon. The RA Officer uses a token distinct from the token used for normal user access.
- The RA workstation will be restricted to only those network accounts associate to the authorized RA Officers, SAs, and IAOs. All other network accounts will not be able to authenticate to the network via the RA workstation.
- RA workstation system and software updates will be applied via a DAA approved Windows Server Update Service (WSUS) server, Windows System Management Server (SMS), System Center Configuration Manager (SCCM) or Windows Update. If used, Windows Update will be configured to retrieve and install critical security updates on a daily basis. If SCCM is available it should be used in preference over SMS.
- Remote access to the RA workstation via SMS, SCCM or Remote Desktop, formerly known as Windows Terminal Services (WTS), will be restricted to authorized SAs of the RA workstation for the purposes of remote maintenance only. TELNET and file transfer protocol (FTP) will not be used or enabled at the RA workstation.
- When static IP addresses are not used, Dynamic Host Configuration Protocol (DHCP) will be used to assign IP addresses in accordance with NSA guidance [NSADHCP], particularly with regard to lease expiration. All external DHCP requests are blocked at the boundary protection NPE(s) unless secure remote access is authorized using a VPN. All addresses, once assigned, are reserved and associated with the MAC address of the workstation network interface. The DHCP Server is configured to record detection of any address it did not issue.

All network service applications will be implemented and used in accordance with the appropriate NSA guidance as provided at http://www.nsa.gov/ia/guidance.

Network protocols not required for RA operations or remote administration are disabled on the RA workstation. TELNET and File Transfer Protocol are not enabled.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

RA hardware and software is procured using standard CC/S/A workstation procurement processes and is not identified for RA use until after delivery.

There is no specific government developed software on RA workstations.

6.6.2 Security Management Controls

RA hardware and software is dedicated to the RA's PKI function. Only applications, hardware devices, network connections, and software necessary for RA operations are installed. Software Restriction Policy is enabled on Windows XP and later version of Windows operating systems and configured to lock the system down to only the approved applications.

The local network operations' formal configuration control system is used to document and control the configuration and modifications of the RA workstation and software.

The IAO verifies that there have been no unauthorized modifications made to the RA system as part of the monthly audit reviews.

If a virus or unauthorized software is detected, all operational use of the workstation is halted, the IAO and RA Officer are immediately notified, and the IAO takes immediate action to address the problem.

6.6.3 Life Cycle Security Controls

RA software is loaded using the DAA approved master disk.

Data on RA equipment will be scanned for malicious code on first use and periodically afterward.

RA hardware and software is procured using standard CC/S/A workstation procurement processes and is not identified for RA use until after delivery. Logical access is recorded as specified in Section 5.4.1. Physical access requirements are addressed in Section 5.1.2.

There is no RA specific software. RA hardware and software updates are procured using standard CC/S/A processes and are not identified for RA use. Installation is done by the RA's system administrator as specified for the update.

6.7 NETWORK SECURITY CONTROLS

RA equipment except the RA token is classified as SECRET as it resides on the SIPRNET.

RA equipment only has the services, ports, and protocols enabled that are required to perform RA functions.

The enclave boundary protection is configured to reject a packet originating outside the network that is using an address from the range used by internal networks.

The RA equipment is protected by the local enclave Intrusion Detection System and firewall. The firewall is configured in accordance with NSA 60 Minute Guide to Network Security, limit services allowed to and from the RA equipment to those required to perform CMA functions and has the following security features:

- Audit of security events;
- Protection of security audit log;
- Identification & Authentication with Secure Action Upon Authentication Failure;

- No data is communicated with Network Intrusion Detection System (IDS) components;
- All communications from any external source flows through the firewall and the firewall implements self-protection; and,
- Ability to filter packets based on source, destination, and port number.

6.8 TIME STAMPING

Not applicable.

7 CERTIFICATE, CRL, AND OCSP PROFILES

Not applicable.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

The DoD PKI Program office conducts an annual audit of all RAs.

The NSS PKI PMA and NSS PKI Member Governing Body may require aperiodic compliance audits of CASs, RAs, or TAs operating under [CNSSI 1300]. The NSS PKI PMA or Member Governing Body is required to state the reason for any aperiodic compliance audit.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The RA Compliance Auditor is selected by the DoD PKI PMO to meet all requirements of Sections 8.2 and 8.3 of [CNSSI 1300]. CC/S/As may nominate a Compliance Auditor to the PKI. The nomination provides the identity of the proposed Compliance Auditor and sufficient information to allow the PMO to determine the qualifications and independence of the auditor as required in Sections 8.2 and 8.3 of [CNSSI 1300].

8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY

The RA auditor is selected/approved by the DoD PKI PMO to meet all requirements of Sections 8.2 and 8.3 of [CNSSI 1300].

8.4 TOPICS COVERED BY ASSESSMENT

8.4.1 Initial Compliance Audit

Not applicable.

8.4.2 Full Compliance Audit

The RA compliance auditor verifies that the RA properly implements all applicable portions of the RA’s approved RPS. The auditor is also required to verify that the RA has a means to assure the quality of the services provided (e.g., periodic customer surveys).

The audit report content is the responsibility of the compliance auditor and should conform to the requirements for [CNSSI 1300].

8.4.3 Alternative Review

Not applicable.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Compliance audit actions taken as a result of the audit are the responsibility of the compliance auditor and should conform to the requirements for [CNSSI 1300].

If any substantive or critical discrepancies are found, the DoD PKI PMO determines if RA will receive a follow-up audit to confirm the implementation and effectiveness of the remedy.

8.6 COMMUNICATION OF RESULTS

The communication of results is the responsibility of the compliance auditor and should conform to the requirements for [CNSSI 1300].

The compliance auditor should also provide a copy to the audited RA and the head of the organization under which the RA operates.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

Not applicable.

9.1.4 Fees for Other Services

RAs do not charge for services.

9.1.5 Refund Policy

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

See [CNSSI 1300].

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.2.4 Fiduciary Relationships

See [CNSSI 1300].

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Business Confidential Information

Not applicable. See Section 9.4 for privacy requirements.

9.3.2 Information Not Within the Scope of Business Confidential Information

Not applicable. See Section 9.4 for privacy requirements.

9.3.3 Responsibility to Protect Business Confidential Information

Not applicable. See Section 9.4 for privacy requirements.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

Not applicable.

9.4.2 Information Treated as Private

Not applicable.

RA Officers and TAs keep secure all personally identifying information that is collected but not included in certificates from unauthorized disclosure. RA Officers and TAs handle all such information as sensitive, and restrict access to those with an official need-to-know in order to perform their official duties.

Private keys associated with signature certificates are always under the control of the PKI Sponsor. Private keys associated with encryption certificates are generated on the CA, inserted into the subscriber token and placed in escrow. Copies of these keys are only provided and controlled as specified in Section 4.12.2. Private keys never appear in unencrypted form outside an approved cryptographic module.

9.4.3 Information Not Deemed Private

Not applicable.

9.4.4 Responsibility to Protect Private Information

See Section 4.12 for information on release of private keys.

RA Officers and TAs keep secure all personally identifying information that is collected but not included in certificates from unauthorized disclosure. RA Officers and TAs handle all such information as sensitive, and restrict access to those with an official need-to-know in order to perform their official duties.

The RA limits access to information on the reason for actual or potential revocations to the parties involved, auditors and appropriate command authorities.

9.4.5 Notice and Consent to Use Private Information

Not applicable.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Not applicable.

TAs refer all requests to the RA. RA Officers refer all requests to the CA which is responsible for processing information requests.

9.4.7 Other Information Disclosure Circumstances

Not applicable.

9.5 INTELLECTUAL PROPERTY RIGHTS

Not applicable.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CAS Representations and Warranties

Not applicable.

9.6.2 RA Representations and Warranties

An RA Officer that performs registration functions as described in this RPS is required to comply with the stipulations of [CNSSI 1300], and comply with the provisions of an RPS approved by the appropriate ANMA for use with [CNSSI 1300]. An RA Officer who is found to have acted in a manner inconsistent with these obligations is subject to revocation of the RA certificate, termination of RA responsibilities by the sponsoring agency, and potentially adverse administrative or disciplinary action under Agency regulations. An RA Officer supporting [CNSSI 1300] is required to conform to the stipulations of this document, including the following:

- Maintaining its operations in conformance with this RPS;
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate; and,
- Ensuring that obligations are imposed on PKI Sponsors in accordance with Section 9.6.3, and that PKI Sponsors are informed of the consequences of not complying with those obligations.

9.6.3 PKI Sponsor Representations and Warranties

As specified in Section 4.4.1, prior to being able to make effective use of a PKI certificate, the PKI Sponsor sign’s an acknowledgement of responsibilities related to protection of the private key and use of the certificate.

PKI Sponsors are required to do the following:

- Accurately represent themselves in all communications with NSS PKI authorities;

- Protect their private keys at all times, in accordance with [CNSSI 1300], as stipulated in their certificate acceptance agreements, and local procedures;
- Promptly notify an RA Officer or TA upon suspicion of loss or compromise of their private keys—such notification is made directly or indirectly through mechanisms consistent with the CAS's CPS;
- Promptly notify an RA Officer or TA of any changes to the information contained in their certificates;
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates; and,
- Upon notification of the recovery of an escrowed private key, determine if revocation of the associated certificate is necessary, and request the revocation if needed.

9.6.4 Relying Party Representations and Warranties

See [CNSSI 1300].

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 Repository Representations and Warranties

Not applicable.

9.6.5.2 NSS PKI PMA

Not applicable.

9.6.5.3 ANMA

Not applicable.

9.6.5.4 Agency POC

Not applicable.

9.7 DISCLAIMERS OF WARRANTIES

RA Officers operating under this RPS, [CAS CPS] and [CNSSI 1300] may not disclaim any responsibilities described in these documents.

9.8 LIMITATIONS OF LIABILITY

Not applicable.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

This RPS becomes effective when approved by the ANMA. It remains in effect until either a new RPS is approved by the ANMA or the ANMA terminates all RAs operating under it.

9.10.2 Termination

The requirements of this RPS related to archive remain in effect through the end of the archive period for the last certificate issued under this RPS.

9.10.3 Effect of Termination and Survival

The responsibilities for protecting business confidential and personal information, and for protecting intellectual property rights, survive termination of the RA operating under this RPS.

Intellectual property rights are in accordance with the Intellectual Property laws of the United States.

The archive requirements of [CNSSI 1300] remain in effect for this RPS through the end of the archive period for the last certificate issued under this RPS.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Not applicable.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

Changes to this RPS are submitted to the ANMA

9.12.2 Notification Mechanism and Period

Not applicable.

9.12.3 Circumstances under which OID must be Changed

Not applicable.

9.13 DISPUTE RESOLUTION PROVISIONS

Not applicable.

9.14 GOVERNING LAW

Not applicable.

9.15 COMPLIANCE WITH APPLICABLE LAW

Not applicable.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this RPS is incorrect or invalid, the other sections shall remain in effect until the RPS is updated. The process for updating this RPS is described in Section 9.12.1. Responsibilities, requirements, and privileges of this document are merged to the newer edition upon release of that newer edition.

9.16.4 Enforcement (Attorney’s Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.

APPENDIX A. REFERENCES

The following documents are referenced in this RPS:

ABA DSG	American Bar Association, *Digital Signature Guidelines*, August 1996.
CNSSI 1300	Committee on National Security Systems Instruction No. 1300, *Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy*, Version 1.1, June 2011.
CNSSI 4009	Committee on National Security Systems Instruction No. 4009, *National Information Assurance (IA) Glossary*, June 2006.
CNSS 014-2010	CNSS National Manager, *Approval of Continued Use of SC650 Token – DECISION MEMORANDUM*, February 2010.
CAS CPS	*National Security Systems (NSS) Public Key Infrastructure (PKI): Department of Defense (DoD) Subordinate Certification Authority (CAS) Certification Practice Statement (CPS),* DoD PKI PMO, V1, 18 March 2010.
DD FORM 2841	*Department of Defense Public Key Infrastructure Registration Official Certificate of Acceptance and Acknowledgement of Responsibilities*, August 2009.
DD FORM 2842	*Department Of Defense Public Key Infrastructure Subscriber Certificate Of Acceptance and Acknowledgement Of Responsibilities*, August 2009.
FIPS 201	National Institute of Standards and Technology, Federal Information Processing Standard 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006.
FORM I-9	OMB No. 1615-0047, Form I-9, *Employment Eligibility Verification*, August 2009.
NPE CA CPS	*National Security Systems (NSS) Public Key Infrastructure (PKI): Department of Defense (DoD) NPE Certification Authority System (CAS) Certification Practice Statement (CPS),* DoD PKI PMO, V1, under development.
RFC 1034	Internet Engineering Task Force, RFC 1034, *Domain Names – Concepts and Facilities*, November 1987.
RFC 3647	Internet Engineering Task Force, RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, November 2003.
RFC 3986	Internet Engineering Task Force, RFC 1034, *Uniform Resource Identifier (URI): Generic Syntax*, January 2005.
RFC 5322	Internet Engineering Task Force, RFC 5322, *Internet Message Format*, October 2008.
SP 800-57	National Institute of Standards and Technology, Special Publication 800-57, *Recommendation for Key Management – Part 1: General*, March 2007.

APPENDIX B. ACRONYMS

The following acronyms are used in this RPS:

ANMA	Agency NSS PKI Management Authority
CA	Certification Authority
CAA	Certification Authority Administrator
CAC	Common Access Card
CAS	Certification Authority System
CC/S/A	Combatant Command/Service/Agency
CN	Common Name
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CP	Certificate Policy
CPMWG	Certificate Policy Management Working Group
CPS	Certification Practice Statement
CRI	Certificate Registration Instructions
CRL	Certificate Revocation List
CSAA	Code Signing Attribute Authority
CSOR	Computer Security Objects Register
CSS	Certificate Status Server
DEERS	Defense Enrollment Eligibility Reporting System
DITPR	Defense Information Technology Portfolio Repository
DN	Distinguished Name
DoD	Department of Defense
EDIPI	Electronic Data Interchange Personal Identifier
FIPS	Federal Information Processing Standard
GUID	Globally Unique Identifier
HTTP	Hyper Text Transfer Protocol
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
ID	Identification
IDS	Intrusion Detection System
IP	Internet Protocol
ITU	International Telecommunications Union
KES	Key Escrow System
LDAP	Lightweight Directory Access Protocol

LRA	Local Registration Authority
NPE	Non-Person Entity
NSA	National Security Agency
NSS PKI	National Security Systems PKI
NVO	NPE Verifying Official
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PCC	Personnel Category Code
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PMO	Program Management Office
POC	Point of Contact
RA	Registration Authority
RFC	Request For Comment
RPS	Registration Practice Statement
SA	System Administrator
TA	Trusted Agent
TLS	Transport Layer Security
TPS	Token Processing System
UPN	User Principle Name
UID	Unique Identifier
UPS	Uninterruptible Power Source
U.S.	United States

APPENDIX C. DEFINITIONS

Term	Definition
Agency NSS PKI Management Authority (ANMA)	The entity within an agency that operates a CA under this policy that is responsible for all aspects of management of the NSS PKI program for that agency, and for participating in the NSS PKI Member Governing Body.
Agency NSS PKI Point of Contact (POC)	The entity within an agency that does not operate a CA under this policy but that obtains certificates from a Common Services Provider CA operated under this policy. The POC is responsible for all aspects of management of the NSS PKI program for that agency and is responsible for participating in the NSS PKI Member Governing Body.
Agency Repository	A repository maintained by each agency that operates a CA. The repository shall support HTTP or LDAP to provide CA certificates and CRLs and collects information from the central repository for use by systems on that agency's network.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [CNSSI 4009]; A process used to confirm the identity of a person or to prove the integrity of specific information
Bits of Security	See Security Strength.
Central Repository	A repository that provides CA certificates and CRLs that supports overall NSS PKI operations with both HTTP and LDAP interfaces. The central repository function may consist of one or more repositories to support overall NSS PKI operations at the discretion of the NSS PKI Member Governing Body or the PMA. The central repository shall collect necessary information from the agency repositories.
Certificate	A digital representation of information which at least • Identifies the certification authority issuing it; • Names or identifies its Subscriber; • Contains the Subscriber's public key; and, • Identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABA DSG]
Certification Authority (CA)	An entity authorized to create, sign, and issue public key certificates.
Certification Authority System (CAS)	The collection of hardware, software, and operating personnel that create, sign, and issue public key certificates to Subscribers.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. [RFC 3647]
Certificate Policy OID	The certificate policy object identifier (OID) is a numeric string that is used to uniquely identify the set of certificate policy requirements stipulated in a CP.
Certificate Revocation List (CRL)	These are digitally signed "blacklists" of revoked certificates. CAs periodically issue CRLs, and users can retrieve them on demand via repositories.
Certificate Status Server (CSS)	An authority that provides status information about certificates on behalf of the CA through online transactions (e.g., an Online Certificate Status Protocol (OCSP) responder).

Term	Definition
Certification Practice Statement (CPS)	A document representing a statement of practices a CA employs in issuing certificates.
CNSS	Committee on National Security Systems, a U.S. government organization providing guidance for the security of national security systems.
Code Signing Certificate	A certificate issued for the purpose of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed by use of a cryptographic hash.
Common Services Provider	A provider of services, typically CA services, to agencies that do not operate their own CA.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [CNSSI 4009]
Content Signing Certificate	A certificate issued for the purpose of digitally signing information (content) to confirm the author and guarantee that the content has not been altered or corrupted since it was signed by use of a cryptographic hash.
Cross Certificate	A certificate issued from a CA that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs. (Note: This is a more narrow definition than described in X.509.)
Encryption Certificate	A certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate.
Identity Certificate	A certificate that provides authentication of the identity claimed. Within the NSS PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures.
Integrity	Protection against unauthorized modification or destruction of information. [CNSSI 4009]
Intermediate Certification Authority (CA)	A CA that is signed by a superior CA (e.g., a Root CA or another Intermediate CA) and signs CAs (e.g., another Intermediate or Subordinate CA). The Intermediate CA exists in the middle of a trust chain between the Trust Anchor, or Root, and the subscriber certificate issuing Subordinate CAs.
Key Compromise	Disclosure of the private key to unauthorized persons, or a violation of the security policy of the PKI in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of the private key may have occurred.
Key Escrow	The retention of the private component of the key pair associated with a Subscriber’s encryption certificate to support key recovery.
Key Escrow System (KES)	The system responsible for storing and providing a mechanism for obtaining copies of private keys associated with encryption certificates, which are necessary for the recovery of encrypted data.
Key Recovery	The process for obtaining a copy of an escrowed private key from the KES.
Legacy NSS PKI	An operational PKI on an agency’s classified network prior to the establishment of the NSS PKI.
Local Registration Authority	A Registration Authority which does not have the authority to take final action on revocation, suspension/restoration, key recovery requests.
Modification	The process of creating a new certificate with a new serial number that differs in one or more fields from the old certificate. The new certificate may have the same or different subject public key.

Term	Definition
Name Subscriber	A Name Subscriber is an individual (i.e., person) whose name appears as the subject in a certificate. The Name subscriber is tightly coupled with the name certificate in which they are named.
NSS PKI	A Public Key Infrastructure (PKI) for SECRET-high collateral classified networks.
NSS PKI Member Governing Body	The organization established from the participating agencies to assist the PMA and provide governance and oversight to the NSS PKI.
PKI Sponsor	A person who is responsible for the private key associated with a certificate and who asserts that the certificate and associated private key are being used in accordance with this CP.
Policy Management Authority (PMA)	Individual or body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Private Key	A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.
Public Key	A mathematical key that has public availability and that applications use to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can encrypt messages or files that the corresponding private key can then decrypt.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity authorized by the CAS to collect, verify, and submit information provided by potential Subscribers which is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function.
Registration Authority (RA) Officer	A trusted role, performed by an individual who is responsible for any of the duties of certificate issuance, certificate revocation, or key recovery.
Registration Practice Statement (RPS)	A document representing a statement of practices an RA employs when performing RA duties for a CAS.
Re-Key	The process of creating a new certificate with a new validity period, serial number, and public key while retaining all other Subscriber information in the original certificate
Relying Party	An entity that relies on the validity of the binding of the Subscriber’s name to a public key to verify or establish the identity and status of an individual, role, or system or device; the integrity of a digitally signed message; the identity of the creator of a message; or confidential communications with the Subscriber
Renewal	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABA DSG]
Restoration	The process of changing the status of a suspended (i.e., temporarily invalid) certificate to valid.
Revocation	The process of permanently ending the binding between a certificate and the identity asserted in the certificate from a specified time forward.

Term	Definition
Role Subscriber	A Role Subscriber is a role, group, or organization whose name appears as the subject in a certificate.
Root Certificate Authority (CA)	The CA that issues the first certificate in a certification chain.
Security Auditor	A trusted role that is responsible for auditing the security of CASs and RAs, including reviewing, maintaining, and archiving audit logs and performing or overseeing internal audits of CASs and RAs.
Security Strength	A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system. In this policy, security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256}. [SP 800-57]
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than authenticating, encrypting data, or performing any other cryptographic functions.
Subordinate Certificate Authority (CA)	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABA DSG]
Suspension	The process of changing the status of a valid certificate to suspended (i.e., temporarily invalid)
System or Device Certificate	A System or Device certificate contains a system or device name as the subject. Examples of systems or devices are workstations, guards, firewalls, routers, web server, database server, and other infrastructure components
System or Device Subscriber	A System or Device Subscriber is the system or device whose name appears as the subject in a certificate.
Technical Non-Repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
Trusted Agent (TA)	An individual explicitly aligned with one or more RA Officers who has been delegated the authority to perform a portion of the RA functions. A TA does not have privileged access to CAS components to authorize certificate issuance, certificate revocation, or key recovery.

APPENDIX D. NOMINATION OF AGENCY REGISTRATION AUTHORITY OFFICER

MEMORANDUM FOR: Defense Information Systems Agency
DoD Public Key Infrastructure Program Management Office
6910 Cooper Avenue
Ft. Meade, MD 20755-7088

SUBJECT: Designation of NSS PKI Registration Authority Officer for ______________________________
(name of organization)

REFERENCES: (a) CNSS Instruction (CNSSI) No. 1300, Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25

(b) ____
(PMO Memo approving the Organization to use the DoD RPS)

1. In accordance with References (a) and (b), the following individuals are hereby designated as Registration Authority (RA) Officer for the above named organization/network. They are charged with executing the responsibility of an RA Officer as set forth in Reference (a) and the Registration Practice Statement (RPS) identified in Reference (b).

   Name:

   RA Officer functions: ( ) Registration/Revocation/NPE Verifying Official ( ) Key Recovery

   Grade/Rank:

   Unique Identification Number (EDIPI/UID):

   Email:

   Telephone (commercial & DSN):

   Mailing Address:

   (Repeat above for each designee.)

2. I have verified that the person or persons nominated for this trusted role meets all of the requirements of Section 5.3.1 of Reference (a).

3. This authority is rescinded when an individual is relieved of duties or leaves the Agency whichever occurs first.

4. If additional information or assistance is required, the point of contact for this action is as follows:

   Point of Contact:

   Phone number:

____
Director
(CC/Service/Agency)

APPENDIX E. NOMINATION OF LOCAL REGISTRATION AUTHORITY/NON-PERSON ENTITY VERIFYING OFFICIAL

FROM: Local Nominating Command/Organization

TO: ________________________________ Registration Authority
(name of organization)

SUBJECT: Designation of NSS Local Registration Authority (LRA)/Non-Person Entity (NPE) Verifying Official (NVO) for ____________________________
(name of organization)

REFERENCES: (a) CNSS Instruction (CNSSI) No. 1300, Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25

(b) ____
(PMO Memo approving the Organization to use the DoD RPS)

1. In accordance with References (a) and (b), the following individual(s) are hereby designated as Local Registration Authorities (LRAs)/Non-Person Entity (NPE) Verifying Official (NVO) for the above named organization. They are charged with executing the responsibility of an LRA/NVO as set forth in Reference (a) and the Registration Practice Statement (RPS) identified in Reference (b).

   Name:

   RA Officer functions: ( ) Registration ( ) NPE Verifying Official

   Grade/Rank:

   id-CNSS-hardware Name Identity CN (e.g., last-name. first-name.initial.EDIPI):

   Email:

   Telephone (commercial & DSN):

   Mailing Address:

   (Repeat above for each designee.)

2. I have verified that the person or persons nominated for this trusted role meets all of the requirements of Section 5.3.1 of Reference (a).

3. This authority is rescinded when an individual is relieved of duties or leaves the Agency whichever occurs first.

4. If additional information or assistance is required, the point of contact for this action is as follows:

   Point of Contact:

   Phone number:

____
Director
(CC/Service/Agency Organization)

APPENDIX F. DESIGNATION OF TRUSTED AGENT

Prepare a Memo on organizational letterhead.

MEMORANDUM FOR: ________________________________ RA or LRA
(name of organization)

SUBJECT: Designation of Trusted Agent (TA) for ________________________________
(name of organization)

REFERENCE: (a) ____
(PMO Memo approving the Organization to use the DoD RPS)

1. The following individual(s) is/are hereby designated as a Trusted Agent(s) for the above named organization. She/he/they is/are charged with executing the responsibilities of a Trusted Agent as stipulated in Section 5.2.1. 3 of the Registration Practice Statement (RPS) specified in Reference (a) for the NSS Public Key Infrastructure.

(Additional responsibilities deemed appropriate at the local level may be stipulated here.)

Name (enter designee name(s) exactly as on their photo ID card):

Grade/Rank:

id-CNSS-hardware Name Identity CN (e.g., last-name.first-name.initial.EDIPI):

Email (use SMTP E-mail address for their .mil account):

Telephone (commercial & DSN):

(Repeat above for each designee.)

2. I have verified that the person or persons nominated for this trusted role meets all of the requirements of Section 5.3.1 of the RPS specified in Reference (a).

3. I understand this designation must be rescinded when an individual is relieved of duties or leaves the organization.

4. My point of contact for additional information or assistance regarding this (these) appointment(s) is name, position, phone (commercial/DSN):

____
Name

____
Title (i.e., Commander, Director, or designee)

APPENDIX G. ACKNOWLEDGEMENT OF TRUSTED AGENT RESPONSIBILITIES

I acknowledge that I have received training to act as a Trusted Agent for the National Security System (NSS) Public Key Infrastructure (PKI) Program. I understand that as a Trusted Agent I will be responsible for the following:

- Validation that the Subscriber is eligible to be registered (U.S. Military, DoD civilian, contractor or others using government furnished equipment and working in government spaces).
- Gathering and forwarding Subscriber registration information to the Registration Authority (RA)/Local Registration Authority (LRA).
- Delivering Certificate Registration Instructions (CRI) and initialized tokens or keyed tokens and/or activation data to Subscribers.
- Verifying the identity of each Subscriber as specified in Section 3.2.3 of the DoD Registration Practice Statement (RPS).
- Assist Subscribers in the downloading and installation of their certificates.
- Reporting to the RA/LRA if a Subscriber suspects a compromise or loss of a private key.
- Abiding by all of the applicable requirements of the DoD Registration Practice Statement (RPS) and executing the responsibilities listed in Section 5.2.1. 3.

Trusted Agent Name: ____

Signature: ____

Unit/Organization: ____

ID Type (Military, Installation Pass): ______________________________

Photo ID Number: ____

Verification of Trusted Agent Identity: I have verified the identity of the person named above by physically checking an U.S. Government issued Photographic Identification Card.

Name of Verifier: ____

Signature: ____

Unit/Organization: ____

Duty Position (LRA, Commander): ________________________________

Date: ____________________

APPENDIX H. PROCEDURE FOR GETTING THE INITIAL TA'S IN PLACE AT LOCATIONS REMOTE FROM AN ESTABLISHED RA/TA

1. The RA Officer, who will oversee the operations of the remote TA, is advised of the need to establish a TA at a location where no NSS PKI RA or TA is currently available.

2. The RA Officer sends a request to the organization commander/director or their designee to identify two people who can be trained to perform the Identification and authentication functions of a TA. The qualifications required of the TA are included in the request. The RA Officer also informs the commander/director that they must complete and verify all information in the Designation of Trusted Agent (No NSS PKI Certificates) memo and send the memo to the RA Officer, as well as obtain a signed Acknowledgement of Responsibilities form from each nominated party, verify the signature on the form is that of the nominated party, and send the form to the RA Officer.

3. The organization commander/director provides a TA nomination memo as shown in Annex 1 of this Appendix.

4. The RA Officer provides instructions to the designated TAs on identity proofing requirements and instructs them to acknowledge their responsibilities using the memo at Appendix G of the RPS, and have the nominating official verify their identity as specified on the form. The form is sent to the RA Officer.

5. Once the RA has the TA acknowledgement of responsibilities from the two nominees, the RA Officer then prepares a CRI for one of the TAs (the PKI Sponsor).

6. If the PKI Sponsor will directly interface with TPS to complete the certificate issuance process:

The RA Officer sends the CRI, wrapped for classified transfer, via continuously accountable means (e.g., US registered Mail with return receipt, FedEx) to the other TA (Authenticating TA) along with an initialized token. The RA Officer emails the Authenticating TA the token serial number and expected arrival date.

Upon receipt, the Authenticating TA validates the PKI Sponsor's identity, executes the DD Form 2842 with the PKI Sponsor and provides the token and CRI to the PKI Sponsor. See Section 4.2.1 of the RPS for procedures if the PKI Sponsor cannot authenticate to the CA using the CRI.

The PKI sponsor executes the certificate issuance process.

The Authenticating TA sends the DD Form 2842 back to the RA Officer.

The Authenticating TA sends an email to the RA Officer, digitally signed with the Authenticating TAs DoD MediumHardware certificate, providing the RA with the Common

Name of the PKI Sponsor's CNSS Signature certificate. The RA Officer verifies that this certificate matches the information in the certificate request.

7. If the RA will interface with TPS to complete the certificate issuance process:

The RA Officer uses the CRI to obtain the certificates.

The RA Officer packages the keyed token in serialized, tamper evident packaging and sends the token to the PKI Sponsor using continuously accountable means (e.g., US Registered Mail with return receipt, Federal Express). The RA Officer sends the PKI Sponsor a digitally signed email with the tamper serial number, the token serial number, and expected delivery date.

Upon receipt of the package the PKI Sponsor inspects it. If the package is not received within a reasonable amount of time or the PKI Sponsor or Authenticating TA has reason to believe the private keys may have been compromised (e.g., a problem with the tamper evident packaging), the Authenticating TA will notify the RA Officer. The RA Officer will investigate and take appropriate steps to resolve the situations, possibly including revoking the certificates and regenerating the keys and certificates. The PKI Sponsor informs the Authenticating TA of receipt and they execute the identity proofing and DD Form 2842.

The authenticating TA sends the DD Form 2842 to the RA Officer.

Upon receipt of the PKI Sponsor's DD Form 2842, the RA Officer sends the PIN, wrapped for classified transfer, to the PKI Sponsor via continuously accountable means.

8. The PKI Sponsor now assumes the role of TA and supports the issuance of certificates to the Authenticating TA and others through the normal process.

ANNEX 1. DESIGNATION OF TRUSTED AGENT (NO NSS PKI CERTIFICATES)

Prepare a Memo on organizational letterhead.

MEMORANDUM FOR: ________________________________ RA or LRA
(name of organization)

SUBJECT: Designation of Trusted Agent (TA) for ________________________________
(name of organization)

REFERENCE: (a) ____
(PMO Memo approving the Organization to use the DoD RPS)

1. The following individual(s) is/are hereby designated as a Trusted Agent(s) for the above named organization. She/he/they is/are charged with executing the responsibilities of a Trusted Agent as stipulated in Section 5.2.1.3 of the Registration Practice Statement (RPS) specified in Reference (a) for the NSS Public Key Infrastructure.

(Additional responsibilities deemed appropriate at the local level may be stipulated here.)

Name (enter designee name(s) exactly as on their photo ID card):

Grade/Rank:

DoD PKI MediumHardware Certificate CN (e.g., last-name.first-name.initial.EDIPI):

Email (use SMTP E-mail address for their .mil account):

Telephone (commercial & DSN):

Mailing Address:

(Repeat above for each designee.)

5. I have verified that the person or persons nominated for this trusted role meets all of the requirements of Section 5.3.1 of the RPS specified in Reference (a).

6. I understand this designation must be rescinded when an individual is relieved of duties or leaves the organization.

7. My point of contact for additional information or assistance regarding this (these) appointment(s) is name, position, phone (commercial/DSN):

____
Name

____
Title (i.e., Commander, Director, or designee)